|  |  |
| --- | --- |
| **Assemblée mondiale de normalisation des télécommunications (AMNT-20)Genève, 1er-9 mars 2022** |  |
|  |  |
|  |  |
| **SÉANCE PLÉNIÈRE** | Document 20-F |
|  | **Décembre 2021** |
|  | **Original: anglais** |
|  |
| Commission d'études 17 de l'UIT-T |
| Sécurité |
| rapport de la CE 17 de l'UIT-T À l'assemblÉe mondiale de normalisation des tÉlÉcommunications (AMNT‑20),partie iI: QUESTIONS qu'il est proposÉ d'Étudier pendant la pÉriode d'Études 2022-2024  |
|  |

|  |  |
| --- | --- |
| **Résumé:** | On trouvera dans la présente contribution le rapport de la Commission d'études 17 de l'UIT-T à l'AMNT-20 concernant ses activités pendant la période d'études 2017-2021. |
| **Contact:** | Heung Youl YoumPrésident de la CE 17 de l'UIT-TCorée (République de) | Courriel: hyyoum@sch.ac.kr |

Note du TSB:

Le rapport de la Commission d'études 17 à l'AMNT‑20 est présenté dans les documents suivants:

Partie I: **Document 19** – Considérations générales

Partie II: **Document 20** – Questions qu'il est proposé d'étudier pendant la période d'études 2022‑2024

Introduction

Le présent document contient le texte des Questions approuvées par la Commission d'études 17 en vue de leur soumission à l'AMNT-20.

On trouvera dans le Tableau 1 la liste des Questions approuvées par le GCNT lors de sa réunion tenue du 11 au 18 janvier 2021 ainsi que leur correspondance avec l'ensemble des Questions en vigueur.

Tableau 1 – Correspondance entre les Questions de la CE 17 proposées (partie de gauche)
et les Questions précédentes (partie de droite)

| Numéro | Titre de la Question | Statut | Numéro précédent | Titre précédent de la Question |
| --- | --- | --- | --- | --- |
| 1/17 | Stratégie et coordination en matière de normalisation de la sécurité | Suite | 1/17 | Stratégie et coordination en matière de normalisation de la sécurité |
| 2/17 | Architecture de sécurité et sécurité des réseaux | Suite | 2/17 | Architecture de sécurité et sécurité des réseaux |
| 3/17 | Gestion de la sécurité des informations de télécommunication et services de sécurité | Suite | 3/17 | Gestion de la sécurité des informations de télécommunication et services de sécurité |
| 4/17 | Cybersécurité et lutte contre le spam | Suite | 4/17 | Cybersécurité et lutte contre le spam |
| 6/17 | Sécurité des services de télécommunication et de l'Internet des objets | Suite | 6/17 | Sécurité des services de télécommunication et de l'Internet des objets |
| 7/17 | Services applicatifs sécurisés | Suite | 7/17 | Services applicatifs sécurisés |
| 8/17 | Sécurité de l'informatique en nuage et de l'infrastructure des mégadonnées | Suite | 8/17 | Sécurité de l'informatique en nuage et de l'infrastructure des mégadonnées |
| 10/17 | Architecture et mécanismes de gestion des identités et de télébiométrie | Suite | 10/17 | Architecture et mécanismes de gestion des identités et de télébiométrie |
| 11/17 | Technologies génériques (notamment: annuaire, infrastructure de clé publique (PKI), langages formels et identificateurs d'objets) utilisées pour les applications sécurisées | Suite | 11/17 | Technologies génériques (notamment: annuaire, infrastructure de clé publique (PKI), langages formels et identificateurs d'objets) utilisées pour les applications sécurisées |
| 13/17 | Sécurité des systèmes de transport intelligents | Suite | 13/17 | Sécurité des systèmes de transport intelligents |
| 14/17 | Sécurité de la technologie des registres distribués (DLT) | Suite | 14/17 | Sécurité de la technologie des registres distribués (DLT) |
| 15/17 | Sécurité relative aux nouvelles technologies, y compris la sécurité quantique | Suite | 15/17 | Sécurité relative aux nouvelles technologies, y compris la sécurité quantique |

Libellé des Questions

QUESTION 1/17

Stratégie et coordination en matière de normalisation de la sécurité

(Suite de la Question 1/17)

# 1 Motifs

Les menaces contre la sécurité de l'infrastructure des télécommunications et des technologies de l'information et de la communication (TIC) sont toujours de plus en plus complexes. Les efforts déployés au fil des années pour sécuriser l'infrastructure ont été quelque peu fragmentés et ponctuels et n'ont pas permis jusqu'ici d'assurer en temps utile le degré souhaité de protection contre ces menaces. Les attaques et les menaces ont eu des incidences économiques considérables et, de ce fait, les pouvoirs publics et les entités ont subi de nombreuses pertes sur le plan financier et organisationnel. Des efforts intenses, permanents et ciblés sont essentiels pour combattre ces menaces.

Cette initiative est complexe et pour la mener à bien, il est nécessaire qu'un grand nombre d'organisations travaillent sur divers aspects de la sécurité, chacune dans son domaine de compétence et selon son mandat. Les différentes parties prenantes doivent donc se coordonner, collaborer et coopérer, ce qui constitue une tâche extrêmement difficile.

Le domaine de la sécurité est vaste. Les questions relatives à la sécurité concernent la quasi-totalité des aspects des TIC et des réseaux. Pour traiter les exigences de sécurité, il existe diverses méthodes, à savoir:

– Une méthode ascendante, dans laquelle les experts conçoivent des mesures de sécurité pour renforcer et protéger un domaine particulier du réseau en utilisant des contre‑mesures et des techniques spécifiques telles que la biométrie et la cryptographie. Quoique relativement courante, c'est une méthode fragmentée qui conduit souvent à des inégalités dans la détermination et l'application des mesures de sécurité.

– Une méthode descendante, qui est une méthode stratégique et de haut niveau pour traiter les questions relatives à la sécurité. Cette méthode, pour laquelle il faut avoir un aperçu global de la situation, est généralement plus difficile à appliquer. En effet, il est plus difficile de trouver des experts qui connaissent de façon complète chaque partie du réseau et ses exigences de sécurité, que de trouver des experts qui connaissent en détail un ou deux domaines particuliers.

– Une combinaison de la méthode ascendante et de la méthode descendante, des efforts de coordination devant être déployés pour assembler les différents éléments. Il s'est avéré que cette méthode pose souvent de nombreux problèmes lorsque les intérêts et les agendas diffèrent.

La présente Question a conduit à l'élaboration de nombreux documents que l'UIT‑T considère comme essentiels pour promouvoir ses travaux et ses résultats. Ils constituent également de précieuses ressources pour l'UIT et pour les organisations extérieures. Parmi ces documents, on peut citer la feuille de route relative aux normes de sécurité des TIC, le Manuel sur la sécurité, les recueils relatifs à la sécurité et le Rapport technique sur l'utilisation efficace des normes de sécurité. La présente Question permettra de définir une vision et de formuler des propositions quant à la structure organisationnelle de la CE 17. L'objectif de la présente Question sera toujours de coordonner et d'organiser toutes les activités relatives à la sécurité des télécommunications/TIC au sein de l'UIT‑T ainsi que d'élaborer et de mettre à jour des documents pour faciliter la coordination et la diffusion externe. Une méthode descendante relative à la sécurité sera utilisée en collaboration et en coordination avec d'autres Commissions d'études et d'autres organismes de normalisation.

Cette activité vise à cibler davantage les efforts déployés au niveau des projets et des stratégies à la fois au sein de la CE 17 et à l'extérieur. La présente Question vise à renforcer les activités de la CE 17, pour faire en sorte qu'elles s'appuient sur un processus efficace permettant d'élaborer, dans les meilleurs délais, des normes relatives aux télécommunications/TIC qui soient de grande qualité et axées sur les besoins du marché. Elle vise également à répondre aux besoins des pays en développement et des groupes régionaux des Commissions d'études à travers la mise en œuvre de la Résolution 44 (Rév.Hammamet, 2016) de l'AMNT relative à la réduction de l'écart en matière de normalisation.

La stratégie en matière de normalisation de la sécurité est l'un des sujets les plus importants des Questions confiées à la CE 17. Cette dernière doit examiner en quoi l'architecture et la conception de la normalisation de la sécurité peuvent permettre d'améliorer les travaux relatifs aux sujets d'étude, existants et futurs, liés à la sécurité.

Les travaux de la CE 17 sur la sécurité sont fondés sur les Résolutions 2, 7, 11, 18, 32, 40, 44, 50, 52, 54, 58, 64, 65, 67, 73, 75, 76, 77, 78, 80, 84, 86, 89, 90, 92, 93, 94, 96, 97 et 98 de l'AMNT, sur les Résolutions 101, 123, 130, 136, 174, 177, 178, 179, 181, 188, 189, 197, 199, 200, 201, 204, 205 et 206 de la Conférence de plénipotentiaires et sur les Résolutions 30, 34, 43, 45, 47, 63, 67, 69, 79, 80 et 84 de la CMDT.

La CE 17 contribue en outre à la réalisation de la grande orientation C5 du SMSI consistant à "Établir la confiance et la sécurité dans l'utilisation des TIC" et à la réalisation de l'Objectif 2 du Plan d'action de Buenos Aires adopté à la Conférence mondiale de développement des télécommunications de 2017, à savoir: "Infrastructure moderne et sûre pour les télécommunications/TIC: Promouvoir le développement d'infrastructures et de services, et notamment instaurer la confiance et la sécurité dans l'utilisation des télécommunications/TIC".

Rapports techniques relevant de la présente Question au 7 janvier 2022: TR.sec-manual et TR.Suss.

Textes en cours d'élaboration au 7 janvier 2022: X.arch-design.

# 2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

a) Quels sont les résultats attendus pour la présente Question?

b) Quels sont les processus, sujets d'étude, méthodes de travail et délai à prévoir pour obtenir les résultats attendus dans le cadre de la Question?

c) Quels documents de diffusion externe (feuille de route, recueils sur la sécurité, rapports techniques, dépliants, pages web, etc.) devront être élaborés et mis à jour par l'UIT?

d) Quels ateliers sur la sécurité sont nécessaires et comment peut-on les organiser?

e) Quelles mesures faut-il prendre pour nouer des relations efficaces avec d'autres organismes de normalisation afin d'avancer les travaux dans le domaine de la sécurité?

f) Quels sont les principales étapes, les critères de réussite et les indicateurs de performance correspondants?

g) Comment peut-on stimuler l'intérêt des Membres du Secteur et des administrations pour les travaux réalisés dans le domaine de la sécurité et comment peut-on maintenir la dynamique?

h) Comment faire en sorte que les fonctions de sécurité des télécommunications/TIC soient plus adaptées au marché?

i) Comment bien faire comprendre au secteur public et au secteur privé l'importance capitale de la sécurité et la nécessité urgente de protéger les intérêts économiques au niveau mondial, qui dépendent d'une infrastructure des télécommunications/TIC robuste et sécurisée?

j) Quelles activités relatives à la sécurité sont actuellement menées dans d'autres commissions d'études de l'UIT et dans d'autres organismes de normalisation?

k) Comment répondre aux besoins des pays en développement et des groupes régionaux des Commissions d'études à travers la mise en œuvre de la Résolution 44 de l'AMNT?

l) Quelle stratégie de normalisation faut-il adopter pour favoriser une solution de sécurité complète et cohérente dans le domaine des télécommunications?

m) Comment définir la stratégie de normalisation compte tenu des Recommandations existantes en matière de sécurité?

# 3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

a) Faire office de contact principal de la CE 17 pour les questions de coordination en matière de sécurité des télécommunications/TIC.

b) Élaborer et tenir à jour une feuille de route sur la structure organisationnelle qui fournira les grands principes ainsi qu'un plan détaillé du niveau et du domaine d'application de l'étude à mener en matière de sécurité. Cette feuille de route indiquera les différents éléments associés (structure et processus) et les relations qui existent entre eux, ainsi que les organisations participantes et leur rôle. Une distinction doit être établie entre les nouveaux systèmes/réseaux et les systèmes/réseaux existants.

c) Tenir à jour la feuille de route relative aux normes de sécurité des TIC.

d) Tenir à jour les recueils de l'UIT-T relatifs à la sécurité.

e) Fournir une assistance et des contributions au TSB pour la mise à jour du manuel sur la sécurité, publié en tant que rapport technique sur la sécurité dans les télécommunications et les technologies de l'information.

f) Tenir à jour le rapport technique sur l'utilisation efficace des normes de sécurité.

g) Fournir des orientations pour la mise en œuvre des normes de sécurité des télécommunications/TIC.

h) Encourager la coopération et la collaboration entre les groupes travaillant à la normalisation de la sécurité des télécommunications/TIC.

i) Examiner comme il se doit les Recommandations et les notes de liaison des autres Commissions d'études et des autres organismes de normalisation pour évaluer les conséquences sur la coordination en matière de sécurité.

j) Fournir une assistance concernant les efforts déployés pour garantir une coordination efficace en matière de sécurité en cas de besoin.

k) Faciliter les liaisons directes entre des groupes externes et les Commissions d'études appropriées de l'UIT-T.

l) Prendre l'initiative à l'UIT-T d'organiser et de planifier des ateliers et des séminaires sur la sécurité en tant que de besoin.

m) Veiller à participer de manière efficace et efficiente aux efforts de coordination en matière de sécurité déployés avec d'autres organismes.

n) Aider la CE 17 à améliorer l'efficacité de ses travaux (par exemple en créant des gabarits, des outils, des procédures ou des indicateurs de performance).

o) Encourager les autorités nationales et les opérateurs des pays en développement à collaborer au niveau régional afin de mieux contribuer aux activités de la CE 17 de l'UIT‑T conformément au mandat de ladite commission d'études et pour ce qui est de la mise en œuvre des Recommandations de la CE 17 sur la sécurité.

p) Aider la CE 17 à réduire l'écart en matière de normalisation conformément à la Rés. 44 de l'AMNT, à la Rés. 123 de la PP et à la Rés. 47 de la CMDT.

q) Assurer une participation efficace et efficiente aux efforts de coordination déployés par la CE 17 en matière de sécurité pour que les activités menées actuellement par la CE 17 dans le domaine de la sécurité soient prises en compte dans le programme de travail de la CE 17 et que des réponses puissent être apportées aux préoccupations des membres de l'UIT‑T.

r) Élaborer un ensemble complet de documents sur la stratégie en matière de normalisation de la sécurité, comprenant notamment des documents sur l'architecture, afin d'appuyer la normalisation des solutions de sécurité en collaboration avec d'autres organismes de normalisation et avec les Commissions d'études de l'UIT-T.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 17 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>).

# 4 Relations

Grandes orientations du SMSI:

– C5

Objectifs de développement durable:

– 8 ([Travail décent et croissance économique](http://www.un.org/development/desa/disabilities/envision2030-goal8.html))

– 9 ([Industrie, innovation et infrastructure](http://www.un.org/development/desa/disabilities/envision2030-goal9.html))

– 17 ([Partenariats pour la réalisation de l'Objectif](https://www.un.org/development/desa/disabilities/envision2030-goal17.html))

Recommandations:

– Série X et autres Recommandations se rapportant à la sécurité des télécommunications/TIC

Questions:

– Questions 2/17, 3/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17, 14/17 et 15/17 de l'UIT‑T

Commissions d'études:

– UIT‑D; UIT‑R; CE 2, 3, 5, 9, 11, 13, 15, 16 et 20 de l'UIT‑T; GCNT, ainsi que les JCA et groupes spécialisés concernés

Organismes de normalisation:

– Alliance for Telecommunications Industry Solutions (ATIS); Cloud Security Alliance (CSA); Institut européen des normes de télécommunication (ETSI); Institute of Electrical and Electronics Engineers (IEEE); Internet Engineering Task Force (IETF); ISO/CEI JTC 1/SC 6 et SC 27, ISO TC 292, ISO TMB; Organization for the Advancement of Structured Information Standards (OASIS); Projet de partenariat pour la troisième génération (3GPP); Projet 2 de partenariat pour la troisième génération (3GPP2); Asia-Pacific Telecommunity Standardization Program (ASTAP)

Autres organismes:

− Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA); National Institute of Standards and Technology (NIST); one M2M; Regional Asia Information Security Exchange (RAISE) Forum

QUESTION 2/17

Architecture de sécurité et sécurité des réseaux

(Suite de la Question 2/17)

# 1 Motifs

Les Recommandations UIT‑T X.800, X.802 et X.803 traitent de la sécurité dans le contexte des systèmes ouverts. L'architecture de sécurité des systèmes offrant des communications de bout en bout est décrite dans la Recommandation UIT‑T X.805. Un ensemble complet de cadres de sécurité détaillés, couvrant des aspects tels que l'authentification, le contrôle d'accès, la non-répudiation, la confidentialité, l'intégrité, l'audit et les alarmes de sécurité, a été établi (X.810, X.811, X.812, X.813, X.814, X.815 et X.816). Pour offrir une sécurité générique des couches supérieures (GULS), les Recommandations UIT‑T X.830, X.831, X.832, X.833, X.834 et X.835 ont été élaborées. En coopération avec l'ISO/CEI JTC 1/SC 27, les Recommandations UIT‑T X.841, X.842 et X.843 relatives aux objets informationnels de sécurité et aux services de tiers de confiance ont été également établies.

Il est nécessaire de poursuivre les efforts de mise à jour et d'amélioration de ces Recommandations relatives à la sécurité pour répondre aux besoins des nouvelles technologies (par exemple les réseaux de prochaine génération (NGN), les aspects relatifs à la sécurité des réseaux pilotés par logiciel (SDN)/de la virtualisation des fonctions de réseau (NFV), le découpage de réseau (NS), la chaîne de fonctions de service (SFC), l'informatique en périphérie à accès multiple (MEC), l'évolution à long terme/l'évolution de l'architecture système (LTE/SAE), les réseaux IMT-2020/5G et les réseaux ultérieurs, le cadre et l'architecture de sécurité communs des services/applications, l'exploitation de l'intelligence artificielle et de l'apprentissage automatique pour instaurer la confiance et la sécurité dans l'utilisation des TIC, les orientations pour la mise en œuvre technique des systèmes assurant des communications de bout en bout et les réseaux IP) et des nouveaux services. Les Recommandations ci-après rendent compte de ces efforts: les Recommandations X.1035 et X.1036, qui présentent en détail les protocoles d'échange de clé avec authentification par mot de passe et la distribution et l'application des politiques; la Recommandation X.1037, qui contient des lignes directrices sur la sécurité du protocole IPv6, les Recommandations X.1038, X.1042, X.1043 et X.1044, qui établissent des exigences de sécurité etc. concernant les réseaux pilotés par logiciel (SDN) et la virtualisation des fonctions de réseau (NFV), et la Recommandation X.1045, qui vise à faciliter la fourniture de services de sécurité personnalisés sur la base de la chaîne de fonctions de service (SFC).

Du fait de la convergence et de la mobilité, les réseaux des opérateurs de télécommunication et les systèmes d'information associés sont exposés à de nouveaux types de menaces de sécurité. Les attaquants ont besoin de moins de compétences pour aller plus en profondeur dans les réseaux et ont tendance à causer des dégâts plus importants. Les attaques par virus, piratage et déni de service se généralisent et ont des effets négatifs sur les éléments de réseau comme sur les systèmes d'appui.

Les secteurs des télécommunications et de l'informatique sont à la recherche de solutions sécuritaires complètes et rentables qui soient indépendantes de la technologie et protègent une grande variété de réseaux, de services et d'applications. Pour parvenir à de telles solutions dans un environnement multifournisseur, la sécurité du réseau doit être optimisée et s'articuler sur des architectures et des technologies de sécurité normalisées. Compte tenu des menaces contre la sécurité de l'environnement des télécommunications et des progrès réalisés dans le domaine des contre-mesures de protection, il convient d'étudier les nouvelles exigences et solutions de sécurité. Il faut élaborer de nouvelles Recommandations qui indiquent comment combiner les normes sur les technologies et les cadres de sécurité afin de mettre en place des solutions de sécurité complètes pour les nouveaux réseaux et services et pour les nouvelles applications.

Recommandations et Suppléments relevant de la présente Question au 7 janvier 2022: Recommandations X.800, X.802, X.803, X.805, X.810, X.811, X.812, X.813, X.814, X.815, X.816, X.830, X.831, X.832, X.833, X.834, X.835, X.841, X.842, X.843, X.1011, X.1031, X.1032, X.1033, X.1034, X.1035, X.1036, X.1037, X.1038, X.1039, X.1040, X.1041, X.1042, X.1043, X.1044, X.1045, X.1046, X.1047, X.1811 et Suppléments X.Suppl.2, X.Suppl.3, X.Suppl.15, X.Suppl.16, X.Suppl.23 et X.Suppl.30.

Textes en cours d'élaboration au 7 janvier 2022: X.5GSec-ecs, X.5GSec-guide, X.5Gsec-message, X.5Gsec-netec, X.5Gsec-ssl, X.5Gsec-t (X.1812), X.5Gsec-vs, TR.zt-acp et XSTP-5Gsec-RM.

# 2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

a) Comment une solution de sécurité des télécommunications complète et cohérente doit‑elle être définie?

b) Quelle est l'architecture d'une solution de sécurité des télécommunications complète et cohérente?

c) Quel est le cadre d'application de l'architecture de sécurité pour élaborer une nouvelle solution de sécurité?

d) Quel est le cadre d'application de l'architecture de sécurité pour évaluer (et donc améliorer) une solution de sécurité existante?

e) Quelles sont les bases architecturales de la sécurité?

i) Quelle est l'architecture pour la sécurité de bout en bout?

ii) Quelle est l'architecture de sécurité pour les systèmes ouverts?

iii) Quelle est l'architecture de sécurité pour l'environnement mobile?

iv) Quelle est l'architecture de sécurité pour les réseaux en évolution?

v) Quelle est l'architecture de sécurité pour les services applicatifs, en collaboration avec les travaux menés au titre de la Question 7/17?

f) Quelles nouvelles Recommandations relatives aux architectures et cadres de sécurité sont nécessaires pour définir des solutions de sécurité dans l'environnement en évolution?

g) Comment convient-il de structurer les normes architecturales par rapport aux Recommandations existantes sur la sécurité?

h) Comment convient-il de structurer les normes architecturales par rapport aux technologies de sécurité avancées existantes?

i) Comment convient-il de modifier les Recommandations relatives aux cadres de sécurité pour les adapter aux nouvelles technologies et quelles nouvelles Recommandations sont nécessaires?

j) Comment sont appliqués les services de sécurité pour définir des solutions de sécurité?

k) Comment est appliqué le contrôle de l'infrastructure des télécommunications/TIC pour définir des solutions de sécurité?

l) Comment l'intelligence artificielle et l'apprentissage automatique peuvent-ils être exploités pour instaurer la confiance et la sécurité dans l'utilisation des TIC?

m) Quelles sont les nouvelles menaces et quels sont les nouveaux enjeux en termes de sécurité qui découlent des nouvelles technologies de réseau (par exemple SDN, NFV, découpage de réseau, SFC, MEC, LTE/SAE, réseaux IMT-2020/5G et réseaux ultérieurs, etc.)?

n) Quelles sont les exigences de sécurité des réseaux IMT-2020/5G et des réseaux ultérieurs et comment la CE 17 peut-elle y répondre?

o) Quels sont les mécanismes de sécurité communs à adopter pour les nouvelles technologies de réseau?

# 3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

a) Élaborer un ensemble complet de Recommandations relatives aux architectures et cadres de sécurité pour définir des solutions de sécurité normalisées pour les télécommunications, en collaboration avec d'autres organismes de normalisation et Commissions d'études de l'UIT-T.

b) Réaliser des études et élaborer des Recommandations relatives à une architecture de réseau de télécommunication fiable qui intègre les technologies de sécurité avancées.

c) Réaliser des études et élaborer des Recommandations sur la manière dont l'intelligence artificielle (IA) et l'apprentissage automatique (ML) pourraient être exploités pour instaurer la confiance et la sécurité dans l'utilisation des TIC.

d) Mettre à jour et améliorer les Recommandations et Suppléments des séries X.800 et X.103x.

e) Réaliser des études et élaborer des Recommandations sur la sécurité de réseau commune.

f) Examiner les exigences de sécurité des réseaux IMT-2020/5G et des réseaux ultérieurs, coordonner les travaux menés sur ce sujet au titre des différentes Questions de la CE 17, faire en sorte que la CE 17 soit l'unique point de contact concernant la sécurité des réseaux IMT-2020/5G et des réseaux ultérieurs et diriger la recherche et la normalisation pour ce qui est de la sécurité de ces réseaux.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 17 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>).

# 4 Relations

Grandes orientations du SMSI:

– C5

Objectifs de développement durable:

– 8 ([Travail décent et croissance économique](http://www.un.org/development/desa/disabilities/envision2030-goal8.html))

– 9 ([Industrie, innovation et infrastructure](http://www.un.org/development/desa/disabilities/envision2030-goal9.html))

– 11 ([Villes et communautés durables](http://www.un.org/development/desa/disabilities/envision2030-goal11.html))

Recommandations:

– Série X et autres Recommandations se rapportant à la sécurité

Questions:

– Questions 1/17, 3/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17, 14/17 et 15/17 de l'UIT‑T

Commissions d'études:

– CE 2 de l'UIT‑D; GT 6B de l'UIT-R; CE 2, 9, 11, 13, 15 et 16 de l'UIT-T ainsi que la JCA-IMT2020

Organismes de normalisation:

– Alliance for Telecommunications Industry Solutions (ATIS); Institut européen des normes de télécommunication (ETSI); GSM Association (GSMA); Forum for International Irregular Network Access (FIINA); ISO/CEI JTC 1/SC 27 et SC 37; CEI TC 25; ISO TC 12; Internet Engineering Task Force (IETF); Projet de partenariat pour la troisième génération (3GPP)

QUESTION 3/17

Gestion de la sécurité des informations de télécommunication
et services de sécurité

(Suite de la Question 3/17)

# 1 Motifs

Pour les organisations de télécommunication, les informations et les processus d'appui, les installations de télécommunication, les réseaux et les supports de transmission constituent des actifs d'entreprise de télécommunication importants. Pour que les organisations de télécommunication gèrent comme il convient ces actifs d'entreprise et continuent de mener à bien leurs activités dans des conditions satisfaisantes, il est indispensable de gérer la sécurité des informations. C'est la raison pour laquelle on a élaboré la Recommandation UIT‑T X.1051, qui établit un code de bonne pratique pour les contrôles de sécurité des informations, à l'intention des organisations de télécommunication.

Sur la base de ce code de bonne pratique, des aspects détaillés et spécifiques relatifs à la gestion (risques, actifs, gouvernance, cadre de gestion et incidents) ont également été examinés et les bonnes pratiques ont fait l'objet d'un Supplément. Il convient d'étudier plus avant de nouveaux aspects en lien avec la Recommandation UIT‑T X.1051. Dans le même temps, les séries de Recommandations doivent être tenues à jour afin de traiter des questions les plus récentes relatives à la gestion de la sécurité des informations. L'objectif est d'élaborer un ensemble de Recommandations UIT-T relatives à la gestion de la sécurité pour les télécommunications sur la base de la Recommandation UIT-T X.1051.

Parallèlement à l'élaboration de Recommandations sur des aspects détaillés et spécifiques relatifs à la gestion sur la base de la Recommandation UIT‑T X.1051, il convient d'examiner les nouveaux domaines relatifs aux services de sécurité des télécommunications/TIC que sont les services des centres de cyberdéfense (qui comprennent les services des centres d'opérations de sécurité (SOC), les services de sécurité gérés (MSS) et les services des équipes d'intervention en cas d'incident informatique (CIRT)), la gestion du cycle de vie pour les contrôles de sécurité et la gestion efficace des risques et enfin la gestion des informations d'identification personnelle. Pour ces services, de nouvelles mesures globales sont nécessaires. Par ailleurs, ces domaines ne concernent pas uniquement la sécurité des informations mais aussi la cybersécurité. Les études réalisées devraient donc porter tout particulièrement sur les aspects de gestion dans les nouveaux domaines précités liés à la sécurité des informations et à la cybersécurité.

Durant ces études, la collaboration étroite entre l'UIT-T et le JTC 1 de l'ISO/CEI sera maintenue afin d'assurer la compatibilité la plus large possible des solutions de sécurité. Il faut en outre tenir compte de la performance des solutions que de nombreux pays ont élaborées sous la forme de normes nationales.

La présente Question diffère des Questions de la Commission d'études 2 en ce sens que la Commission d'études 2 s'occupe de l'échange des informations de gestion de réseau entre éléments de réseau et systèmes de gestion ainsi qu'entre systèmes de gestion dans l'environnement du réseau de gestion des télécommunications (RGT). La présente Question porte essentiellement sur la protection des actifs d'entreprise, y compris les informations et les processus, en vue de la gestion de la sécurité des informations.

Recommandations et Suppléments relevant de la présente Question au 7 janvier 2022: Recommandations E.409 (conjointement avec la CE 2), X.1051, X.1052, X.1053, X.1054, X.1055, X.1056, X.1057, X.1058, X.1059, X.1060, X.1061 et Suppléments X.Suppl.13, Suppl.27, Suppl.32, Suppl.34 et X.Suppl.36.

Textes en cours d'élaboration au 7 janvier 2022: X.1051rev2.

# 2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

a) Comment identifier les questions spécifiques de gestion de la sécurité pour les organisations de télécommunication?

b) Comment identifier et gérer la mesure de la gestion de la sécurité dans les télécommunications?

c) Comment mettre en correspondance les objectifs de contrôle et les contrôles, et les intégrer aux aspects de gestion et d'exploitation dans les organisations de télécommunication?

d) Comment appliquer les concepts et les principes de gouvernance de la sécurité des informations pour que les organisations puissent évaluer, encadrer, surveiller et diffuser leurs activités liées à la sécurité des informations?

e) Quelles solutions de traitement des risques convient-il d'adopter pour gérer l'impact d'un incident de sécurité?

f) Comment appliquer les bonnes pratiques fournissant des orientations en termes de services de sécurité (par exemple les services CDC, comprenant les services SOC, MSS et CIRT)?

g) Comment mettre en place correctement une gestion de la sécurité des informations pour les organisations de télécommunication, en utilisant les normes existantes (UIT‑T, ISO/CEI, etc.)?

h) Comment mettre en œuvre efficacement la gestion des informations d'identification personnelle?

i) Quelles améliorations convient-il d'apporter aux Recommandations existantes en cours de révision ou aux nouvelles Recommandations en cours d'élaboration pour réduire directement ou indirectement l'impact sur le changement climatique (par exemple économies d'énergie, réduction des émissions de gaz à effet de serre, mise en œuvre de systèmes de surveillance) dans le secteur des télécommunications/TIC ou dans les autres secteurs?

# 3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

a) Étudier et définir un cadre pour les fonctions de gestion de la sécurité des informations décrites dans la Recommandation UIT‑T X.1051.

b) Étudier et définir une méthodologie de mise en place d'une gestion de la sécurité des informations pour les organisations de télécommunication compte tenu des normes existantes (UIT‑T, ISO/CEI, etc.).

c) Étudier et définir un cadre/des lignes directrices pour les services de sécurité, par exemple les services CDC, comprenant les services SOC, MSS et CIRT.

d) Étudier et définir des lignes directrices pour la gestion du cycle de vie des contrôles de sécurité.

e) Étudier et définir des lignes directrices pour une gestion efficace des risques (par exemple, acquisition d'une cyberassurance pour la gestion des risques).

f) Étudier et définir des lignes directrices relatives à la gestion des informations d'identification personnelle.

g) Proposer le plan général de nouvelles Recommandations.

h) Évaluer les résultats des activités ci-dessus par rapport aux possibilités d'utilisation pour les installations et services de télécommunication.

i) Élaborer des projets de Recommandation.

j) Mettre à jour et améliorer les Recommandations de la série X.105x.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 17 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>).

# 4 Relations

Grandes orientations du SMSI:

– C5

Objectifs de développement durable:

– 8 ([Travail décent et croissance économique](http://www.un.org/development/desa/disabilities/envision2030-goal8.html))

– 9 ([Industrie, innovation et infrastructure](http://www.un.org/development/desa/disabilities/envision2030-goal9.html))

Recommandations:

– Séries X.800, X.1000, X.1100, X.1200 et X.1300

Questions:

– Questions 1/17, 2/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17, 14/17, 15/17 et 14/15 de l'UIT-T

Commissions d'études:

– UIT‑D, UIT-R, CE 2, 9, 11, 13, 15, 16 et 20 de l'UIT-T

Organismes de normalisation:

– Asia Pacific Telecommunity Standardization Programme (ASTAP); Institut européen des normes de télécommunication (ETSI); ISO/CEI JTC 1/SC 27; ISO/CEI JTC1 SC40, ISO/TC 68, ISO/TC 215; ISO/TC 307; National Institute of Standards and Technology (NIST); Telecommunication Technology Committee (TTC); Projet de partenariat pour la troisième génération (3GPP); Forum des équipes de sécurité et d'intervention en cas d'incidents (FIRST)

QUESTION 4/17

Cybersécurité et lutte contre le spam

(Suite de la Question 4/17)

# 1 Motifs

Le paysage des télécommunications évolue constamment, tout comme les exigences associées relatives à la sécurité des télécommunications/TIC. Dans le cyberenvironnement, les menaces et les attaques dirigées contre les télécommunications/TIC sont en constante évolution et sont toujours plus sophistiquées et ciblées. Elles causent un large éventail de problèmes aux utilisateurs, fournisseurs de services, opérateurs et réseaux. Il est indispensable de définir des cadres et des exigences en termes de cybersécurité, mais aussi d'élaborer un ensemble de Recommandations basées sur des bonnes pratiques pour permettre aux organisations de gérer les risques de cybersécurité.

Les cadres et les exigences de cybersécurité visant à lutter contre les menaces et les attaques comprendraient un ensemble d'éléments, qui devraient consister à identifier, à protéger, à détecter, à intervenir et à rétablir. Lutter contre les cyberattaques par des moyens techniques nécessite des exigences globales pour: limiter les risques, détecter les incidents et intervenir rapidement pour y remédier; échanger des informations sur la cybersécurité, notamment grâce aux Techniques d'échange d'informations sur la cybersécurité (CYBEX) et à l'expression structurée d'informations sur les menaces (STIX); et sécuriser les protocoles, les infrastructures et les applications qui sont utilisés pour nos communications quotidiennes.

L'intelligence artificielle et l'apprentissage automatique sont appliqués plus largement que jamais à travers les différents secteurs et dans les applications. Les possibilités techniques offertes par l'intelligence artificielle et l'apprentissage automatique devraient permettre d'améliorer la qualité et l'efficacité des activités techniques visant à lutter contre les menaces et les attaques. Les services de sécurité gérés (MSS) sont des services qui ont été sous-traités à un fournisseur. Ils comprennent deux aspects: la technique et la gestion.

Les technologies de cybersécurité assurent un appui technique pour les services de sécurité gérés, la détection et la réponse via les points d'extrémité, la prévention contre les intrusions, la détection de celles-ci et l'identification de la source des attaques, afin de protéger les services et les informations personnelles, y compris les informations d'identification personnelle (PII), et afin de fournir une garantie des informations entre les entités en interaction.

L'échange d'informations sur la cybersécurité grâce aux techniques CYBEX et les renseignements sur les cybermenaces sont essentiels pour protéger les infrastructures de télécommunication/TIC et pour renforcer la cybersécurité au profit des fournisseurs de télécommunication/TIC.

En outre, les cybermenaces évoluent très rapidement et il est donc nécessaire d'examiner les aspects techniques pour renforcer les procédures, les politiques techniques et les cadres de cybersécurité. L'enjeu est d'assurer un niveau minimum d'harmonisation, étant donné que la cybersécurité nécessite une collaboration entre toutes les parties prenantes.

S'agissant des défis liés à la cybersécurité, le spam est devenu un problème de grande ampleur, susceptible d'entraîner un manque à gagner pour les fournisseurs de services Internet, les opérateurs de télécommunications (mobiles également) et les entreprises dans le monde entier. Lorsqu'il est utilisé pour l'hameçonnage et la diffusion de virus, de vers, de logiciels-espions et d'autres formes de logiciels malveillants, le spam crée en outre des problèmes en termes de sécurité des informations et des réseaux de télécommunication. Par conséquent, par sa Résolution 52 (Rév.Hammamet, 2016), l'AMNT a chargé les commissions d'études compétentes de continuer à fournir un appui aux travaux en cours, en particulier à ceux de la Commission d'études 17, concernant la lutte contre le spam et d'accélérer leurs travaux sur le spam afin de traiter le problème des menaces actuelles et futures, dans les domaines de compétence de l'UIT-T, selon qu'il conviendra. Elle les a aussi chargées de poursuivre la collaboration avec les organisations concernées afin de continuer à élaborer, d'urgence, des Recommandations techniques en vue d'échanger de bonnes pratiques et à diffuser des informations dans le cadre d'ateliers organisés conjointement, de séances de formation, etc., et a en outre chargé la Commission d'études 17 de rendre compte régulièrement au Groupe consultatif de la normalisation des télécommunications de la mise en œuvre de cette Résolution.

En raison de l'essor rapide de l'Internet mobile et de la convergence des technologies TIC, les spams utilisent de nouvelles fonctionnalités et constituent donc une menace toujours plus difficile à contrer. Les principales méthodes de spam ont beaucoup évolué, passant des formes classiques de publicités et de fraudes aux logiciels convergents malveillants, utilisés notamment pour obtenir des rançons et mener des attaques ciblées. En outre, les spams de nouvelle génération sont également non sollicités et harcèlent les consommateurs de services TIC, mais sont encore plus nuisibles que les spams classiques. Les attaques ciblées se font souvent via du hameçonnage, une méthode d'ingénierie sociale visant à accéder aux réseaux par des canaux légitimes tels que les courriers électroniques. Le rançongiciel est un type de logiciel malveillant qui menace de publier les données concernant la victime, ou de bloquer l'accès à ces données de manière permanente jusqu'au versement d'une rançon. Certains logiciels malveillants, notamment la plupart des rançongiciels, peuvent être diffusés via des pièces jointes malveillantes dans des courriers électroniques et via des sites web infectés. Du fait de l'évolution de l'intelligence artificielle et de l'apprentissage automatique (AI/ML), certaines communications peuvent être initiées par des ordinateurs et non par des personnes, notamment via les appels et les discussions robotisées, les SMS automatiques etc. Les algorithmes d'intelligence artificielle/d'apprentissage automatique peuvent également permettre d'exploiter les informations personnelles de manière plus poussée, afin de cibler des destinataires pour l'envoi de spams commerciaux à grande échelle ou de spams frauduleux.

Avec le large déploiement des IMT-2020, de l'Internet des objets (IoT) et d'autres technologies de télécommunication/TIC, les spams ont progressivement commencé à toucher les systèmes industriels.

Il a été admis que la lutte contre le spam est un problème de portée mondiale qui appelle une approche tous azimuts et exhaustive. En tant que Commission d'études directrice pour la sécurité des télécommunications et dans le cadre des activités déployées au titre de la Résolution 52 de l'AMNT, la Commission d'études 17 est bien placée pour étudier les diverses mesures techniques susceptibles de faciliter la lutte contre le spam afin d'assurer la stabilité et la fiabilité du réseau de télécommunication. La structure technique des Recommandations existantes et potentielles relatives à la lutte contre le spam par des moyens techniques a notamment été établie afin de faciliter la production de Recommandations. Par ailleurs, il convient de publier de nouvelles Recommandations relatives à la lutte contre les nouvelles formes de spam.

Recommandations, Suppléments et rapports techniques relevant de la présente Question au 7 janvier 2022: Recommandations X.1205, X.1206, X.1207, X.1208, X.1209, X.1210, X.1211, X.1212, X.1213, X.1214, X.1215, X.1216, X.1217, X.1218, X.1231, X.1232, X.1233, X.1234, X.1235, X.1240, X.1241, X.1242, X.1243, X.1244, X.1245, X.1246, X.1247, X.1248, X.1249, X.1303, X.1303bis, X.1500, X.1500.1, X.1520, X.1521, X.1524, X.1525, X.1526, X.1528, X.1528.1, X.1528.2, X.1528.3, X.1528.4, X.1541, X.1542, X.1544, X.1546, X.1550, X.1570, X.1580, X.1581, X.1582, Suppléments X.Suppl.6, X.Suppl.8, X.Suppl.9, X.Suppl.10, X.Suppl.11, X.Suppl.12, X.Suppl.14, X.Suppl.18, X.Suppl.20, X.Suppl.25, X.Suppl.29 et Rapport technique TR.usm.

Textes en cours d'élaboration au 7 janvier 2022: X.1246Amd.1, X.1247Amd.1, X.arc-ev, X.ics‑schema, X.tsfpp et X.Sup-cs-ml.

# 2 Question

Les sujets à étudier dans le contexte des réseaux et des systèmes de télécommunication/TIC sont notamment les suivants (la liste n'est pas exhaustive):

a) Comment les fournisseurs de télécommunications/TIC doivent-ils sécuriser leur infrastructure, maintenir un fonctionnement sécurisé et utiliser des mécanismes de garantie de la sécurité?

b) Quelles sont les exigences de sécurité que les concepteurs et fabricants de logiciels, de protocoles de télécommunication et de systèmes de communication doivent prendre en considération pour concevoir, élaborer et partager des bonnes pratiques dans le cyberenvironnement?

c) Comment partager efficacement les informations sur les vulnérabilités, les failles et les moyens d'attaque pour faciliter le traitement des vulnérabilités?

d) Quelles exigences et solutions sont nécessaires pour garantir la résilience, la sécurité et l'intégrité des systèmes composables dans le domaine des télécommunications/TIC?

e) Quelles exigences et solutions sont nécessaires pour la responsabilisation, l'intervention en cas d'incident, les services de sécurité gérés, l'identification des auteurs des cyberattaques, le suivi des menaces et la communication des risques dans le domaine des télécommunications/TIC?

f) Quels mécanismes sont nécessaires pour le partage d'informations relatives à la garantie de la cybersécurité des systèmes dans le cyberenvironnement, en particulier des systèmes en nuage, imbriqués et composables?

g) Comment utiliser l'intelligence artificielle et l'apprentissage automatique pour déceler et analyser rapidement les nouvelles menaces et vulnérabilités?

h) Comment les fournisseurs de télécommunication/TIC devraient-ils exploiter les renseignements sur les menaces pour renforcer leurs activités en matière de sécurité?

i) Comment peut-on utiliser les réseaux pour assurer des services critiques (par exemple, utilisation du protocole d'alerte commun) de façon sécurisée pendant une situation d'urgence nationale?

j) Quelles sont les composantes des cadres de cybersécurité que les organisations peuvent utiliser pour faire face aux risques?

k) Quelles sont les lignes directrices et bonnes pratiques nécessaires en matière de sécurité afin d'identifier et d'atténuer les cybermenaces et de réduire leur impact, en particulier pour ce qui est des logiciels malveillants, du déni de service réparti et de l'ingénierie sociale?

l) Quels types de rapports techniques et de Recommandations est-il possible d'élaborer pour appuyer les procédures, les politiques techniques et les cadres de cybersécurité?

m) Comment comprendre et identifier le spam?

n) Quelles sont les nouvelles formes de spam dans les réseaux existants et futurs?

o) Quelles sont les graves conséquences du spam?

p) Quels sont les facteurs techniques qui contribuent à rendre difficile l'identification des sources de spam?

q) En quoi les nouvelles technologies, les nouveaux services et les nouvelles applications (messagerie instantanée, réseaux sociaux, applications mobiles, téléphonie LTE (évolution à long terme), services de communication enrichis (RCS), etc.) rendent-ils possibles la création et la diffusion de spams?

r) Comment peut-on identifier les voies d'acheminement, les sources et les volumes des spams pour lutter contre ces derniers?

s) Comment peut-on assurer la sécurité des services de messagerie?

t) Comment peut-on empêcher la diffusion de logiciels malveillants via les courriers électroniques?

u) Comment peut-on identifier les voies d'acheminement, les sources et les volumes des spams et estimer le montant des investissements nécessaires dans les installations et les autres moyens techniques requis pour lutter contre les spams?

v) Comment peut-on prévenir les attaques ciblées par harponnage?

w) Comment peut-on empêcher la diffusion de rançongiciels via les courriers électroniques?

x) Comment peut-on déceler et prévenir les spams recourant aux techniques de communication basées sur l'intelligence artificielle et sur l'apprentissage automatique?

y) Comment protéger les informations personnelles en utilisant les technologies reposant sur l'intelligence artificielle et sur l'apprentissage automatique afin d'empêcher la diffusion des messages de spam?

z) Quelles sont les études techniques déjà entreprises dans le cadre des activités de l'IETF, du 3GPP, de la GSMA, du M3AAWG, et d'autres forums, ainsi que par des entités du secteur privé, pour traiter le problème du spam?

aa) Quels sont les travaux de normalisation sur le réseau de télécommunication éventuellement nécessaires pour lutter efficacement contre le spam et assurer la stabilité et la fiabilité du réseau de télécommunication?

bb) Quelles sont les solutions efficaces et efficientes de lutte contre le spam?

cc) Comment sont définies les exigences génériques et spécifiques pour le partage d'informations sur la lutte contre le spam?

dd) Quelles sont les bonnes pratiques de lutte contre le spam?

# 3 Tâches

Les tâches à envisager dans le contexte des réseaux et des systèmes de télécommunication/TIC sont notamment les suivantes (la liste n'est pas exhaustive):

a) Collaborer avec les Commissions d'études de l'UIT‑T, l'ETSI, le FIRST, l'IETF, l'IEEE, l'ISO/CEI JTC 1, l'OASIS, l'OMA, le TCG, le 3GPP, le 3GPP2, et d'autres organismes de normalisation concernant la cybersécurité.

b) Travailler à l'élaboration de cadres et de Recommandations pour spécifier comment les fournisseurs de télécommunications/TIC peuvent sécuriser leur infrastructure et maintenir un fonctionnement sécurisé, et échanger des informations sur la cybersécurité.

c) Élaborer un ensemble de Recommandations définissant des solutions de sécurité dans le domaine des télécommunications/TIC pour la responsabilisation, la garantie, l'intervention et le rétablissement en cas d'incident, en tenant compte des aspects techniques des services de sécurité gérés.

d) Étudier et spécifier les techniques et capacités de sécurité permettant aux fournisseurs de services de coordonner et d'échanger des informations sur les vulnérabilités, les plates-formes et les cyberattaques.

e) Étudier et spécifier un cadre de cybersécurité comprenant un ensemble d'éléments qui devraient consister à identifier, à protéger, à détecter, à intervenir et à rétablir.

f) Spécifier comment utiliser l'intelligence artificielle et l'apprentissage automatique pour déceler et analyser rapidement les nouvelles menaces et vulnérabilités.

g) Spécifier comment appliquer des mécanismes de responsabilisation, de garantie et d'intervention en cas d'incident dans les réseaux de télécommunication/TIC.

h) Élaborer des lignes directrices et des techniques de protection des informations personnelles et des informations d'identification personnelle (PII) sur la base des techniques CYBEX, STIX et TAXII (échange sécurisé et automatisé d'informations sur les indicateurs) et des outils de sécurité associés.

i) Étudier et élaborer des orientations techniques pour la gestion des menaces via l'identification de la source des cyberattaques.

j) Aider les autres Commissions d'études de l'UIT‑T à appliquer les Recommandations relatives à la cybersécurité pour définir des solutions de sécurité spécifiques.

k) Élaborer des bonnes pratiques et des lignes directrices concernant le partage d'informations sur les vulnérabilités ainsi que des solutions pour faciliter le traitement des vulnérabilités.

l) Collaborer avec les autres organismes de normalisation (par exemple l'OASIS pour inclure les techniques STIX et TAXII dans les documents de l'UIT).

m) Travailler à l'élaboration de Recommandations et de rapports techniques sur la manière de faire face aux problèmes en matière de cybersécurité.

n) Faire office de groupe responsable au sein de l'UIT-T concernant les moyens techniques de lutte contre le spam, celui-ci étant décrit par la Commission d'études 2.

o) Identifier et étudier les risques pour la sécurité du réseau de télécommunication (en périphérie et dans le réseau central) qui résultent de l'évolution constante de la nature du spam.

p) Identifier les voies d'acheminement, les sources et les volumes des spams et estimer le montant des investissements nécessaires dans les installations et les autres moyens techniques requis pour lutter contre les spams.

q) Établir une liste de ressources complète et à jour répertoriant les mesures techniques existantes de lutte contre le spam dans les réseaux de télécommunication qui sont utilisées ou en cours d'élaboration.

r) Élaborer de nouvelles Recommandations relatives à la lutte contre les formes existantes ou nouvelles de spam.

s) Définir un ensemble de mesures techniques pour assurer la sécurité des services de messagerie.

t) Élaborer de nouvelles Recommandations pour empêcher la diffusion de logiciels malveillants via les courriers électroniques.

u) Élaborer un ensemble de solutions pour prévenir les attaques ciblées par harponnage via les courriers électroniques.

v) Élaborer de nouvelles Recommandations pour empêcher la diffusion de rançongiciels via les courriers électroniques.

w) Définir des exigences génériques et spécifiques pour le partage d'informations sur la lutte contre le spam.

x) Établir si de nouvelles Recommandations ou des améliorations apportées à des Recommandations existantes – notamment en ce qui concerne les méthodes permettant de lutter contre la diffusion de courriels non sollicités, de logiciels malveillants et d'autres types de contenus malveillants, et de lutter contre les équipements de réseau compromis, en particulier les botnets – pourraient être utiles dans le cadre des efforts déployés pour lutter efficacement contre le spam et assurer la stabilité et la fiabilité du réseau de télécommunication.

y) Élaborer un ensemble de solutions ou de nouvelles Recommandations pour lutter contre les spams recourant aux techniques de communication basées sur l'intelligence artificielle/l'apprentissage automatique.

z) Fournir régulièrement au Groupe consultatif de la normalisation des télécommunications et au Directeur du Bureau de la normalisation des télécommunications des éléments actualisés, destinés à être incorporés dans le rapport annuel au Conseil.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 17 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>).

# 4 Relations

Grandes orientations du SMSI:

– C5

Objectifs de développement durable:

– 8 ([Travail décent et croissance économique](http://www.un.org/development/desa/disabilities/envision2030-goal8.html))

– 9 ([Industrie, innovation et infrastructure](http://www.un.org/development/desa/disabilities/envision2030-goal9.html))

Recommandations:

– Série X et autres Recommandations se rapportant à la sécurité

Questions:

– Questions 1/17, 2/17, 3/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17, 14/17 et 15/17 de l'UIT-T

Commissions d'études:

– CE 1 et CE 2 de l'UIT‑D; CE 2, 9, 11, 13, 16 et 20 de l'UIT-T

Organismes de normalisation:

– Institut européen des normes de télécommunication (ETSI); Institute of Electrical and Electronics Engineers (IEEE); Internet Engineering Task Force (IETF); CEI TC 57, CEI TC 292, CEI TC 65/WG10; ISO/CEI JTC 1/SC 27; National Institute of Standards and Technology (NIST); Organization for the Advancement of Structured Information Standards (OASIS); Open Mobile Alliance (OMA); Open Group; Object Management Group (OMG); Projet de partenariat pour la troisième génération (3GPP); Projet 2 de partenariat pour la troisième génération (3GPP2); Trusted Computing Group (TCG)

Autres organismes:

– Anti-Phishing Working Group (APWG); CERT/CC; CIRT; Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA); GSM Association (GSMA); Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG); Forum des équipes de sécurité et d'intervention en cas d'incidents (FIRST); National Institute of Standards and Technology (NIST); Organisation de coopération et de développement économiques (OCDE)

QUESTION 6/17

Sécurité des services de télécommunication et de l'Internet des objets

(Suite de la Question 6/17)

# 1 Motifs

La Recommandation UIT‑T X.1101 décrit les exigences de sécurité et le cadre applicables aux communications en multidiffusion. Les Recommandations UIT‑T X.1111, X.1112, X.1113 et X.1114 décrivent le cadre de sécurité, le profil de certificat de dispositif, les mécanismes d'authentification et le cadre d'autorisation pour les réseaux domestiques. Les Recommandations UIT‑T X.1121, X.1122, X.1123, X.1124 et X.1125 indiquent en détail la sécurité pour les réseaux mobiles. Les Recommandations UIT‑T X.1171, X.1311 et X.1312 indiquent respectivement le cadre de confidentialité pour les services NID mobiles, le cadre de sécurité des réseaux de capteurs ubiquitaires, les lignes directrices sur la sécurité des intergiciels des réseaux de capteurs ubiquitaires et les exigences de sécurité pour le routage dans les réseaux de capteurs sans fil. Les Recommandations UIT‑T X.1191, X.1192, X.1193, X.1194, X.1195, X.1196, X.1197 et X.1198 décrivent un ensemble complet d'exigences, mécanismes et cadre pour la sécurité des services de TVIP. Les Suppléments UIT‑T X.Suppl.19 et X.Suppl.24 portent sur les aspects de sécurité des téléphones mobiles. Les Recommandations UIT-T X.1331 et X.1332 et le Supplément UIT‑T X.Suppl.26 portent sur les aspects de sécurité des réseaux électriques intelligents. Les Recommandations UIT-T X.1361, X.1362, X.1363, X.1364 et X.1365 présentent les exigences, les mécanismes et les cadres de sécurité liés à l'Internet des objets. Il faut poursuivre les efforts pour mettre à jour et améliorer ces Recommandations et Suppléments relatifs à la sécurité afin de répondre aux besoins des nouvelles technologies et des nouveaux services.

Les services et les réseaux de télécommunication et l'Internet des objets permettent à n'importe qui d'accéder à n'importe quelle information souhaitée de façon conviviale, à tout moment, en tout lieu et en utilisant n'importe quel type de dispositif. Le secteur des télécommunications connaît une croissance exponentielle dans le domaine des services de télécommunication basés sur la technologie mobile. En particulier, la sécurité des services et des réseaux de télécommunication propres à un domaine entre des dispositifs hétérogènes utilisant des technologies au niveau application telles que l'Internet des objets et les villes intelligentes (y compris les communications de machine à machine (M2M), les applications d'identification par radiofréquence (RFID), les communications en champ proche (NFC) et les réseaux de capteurs), les réseaux domestiques, les systèmes de contrôle industriel (par exemple les usines intelligentes), les réseaux électriques intelligents, le module d'identité d'abonné incorporé (eSIM), les smartphones, les réseaux de TVIP, etc. est indispensable pour le développement futur du secteur, des opérateurs de réseau et des fournisseurs de services.

La normalisation de solutions de sécurité complètes optimales est essentielle pour les opérateurs de réseau et les fournisseurs de services qui travaillent dans un environnement de télécommunication international multifournisseur. En raison de certaines caractéristiques particulières de l'environnement de l'IoT (par exemple, puissance de calcul et taille de mémoire limitées des petits dispositifs mobiles, long cycle de vie, systèmes d'exploitation et logiciels personnalisés), assurer la sécurité et la protection des informations d'identification personnelle (PII) est une tâche particulièrement difficile qui mérite une attention et une étude particulières.

Recommandations et Suppléments relevant de la présente Question au 7 janvier 2022: Recommandations X.1101, X.1111, X.1112, X.1113, X.1114, X.1121, X.1122, X.1123, X.1124, X.1125, X.1126, X.1127, X.1171, X.1191, X.1192, X.1193, X.1194, X.1195, X.1196, X.1197, X.1198, X.1311, X.1312, X.1313, X.1314, X.1331, X.1332, X.1333, X.1361, X.1362, X.1363, X.1364, X.1365, X.1366, X.1367, X.1368, X.1369, X.1453 et Suppléments X.Suppl.19, X.Suppl.24 et X.Suppl.26.

Textes en cours d'élaboration au 7 janvier 2022: X.iotsec-4, X.ra-iot, X.sc-iot, X.ztd-iot et TR.ibc‑cd.

# 2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

a) Comment identifier et définir les aspects relatifs à la sécurité des services de télécommunication et de l'Internet des objets dans le domaine des télécommunications mobiles?

b) Comment identifier et traiter les menaces qui pèsent sur les services de télécommunication et l'Internet des objets?

c) Quelles technologies de sécurité peuvent être utilisées pour les services de télécommunication et l'Internet des objets?

d) Comment assurer et maintenir une interconnectivité sécurisée dans l'Internet des objets et les services de télécommunication?

e) Comment étudier et définir des technologies de sécurité basées sur l'intelligence artificielle/l'apprentissage automatique pour les services de télécommunication et l'Internet des objets?

f) Quelles techniques, quels mécanismes et quels protocoles de sécurité sont nécessaires pour l'Internet des objets et les nouveaux services de télécommunication, en particulier les nouveaux services de protection du contenu numérique?

g) Quelles sont les solutions de sécurité globales pour l'Internet des objets et les services de télécommunication (par exemple les services utilisés pour les villes intelligentes, les réseaux électriques intelligents et les systèmes de contrôle industriel (notamment les usines intelligentes) qui sont fondés sur les réseaux de télécommunication/TIC)?

h) Quelles sont les bonnes pratiques ou lignes directrices relatives à l'Internet des objets et aux services de télécommunication sécurisés?

i) Quelles améliorations convient-il d'apporter aux Recommandations existantes en cours de révision ou aux nouvelles Recommandations en cours d'élaboration pour réduire, directement ou indirectement, l'impact sur le changement climatique (par exemple économies d'énergie, réduction des émissions de gaz à effet de serre, mise en œuvre de systèmes de surveillance) dans le secteur des télécommunications/TIC ou dans les autres secteurs?

j) Quels mécanismes de protection et de gestion des informations d'identification personnelle (PII) sont nécessaires pour l'Internet des objets et les services de télécommunication sécurisés?

# 3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

a) En collaboration avec d'autres Commissions d'études de l'UIT‑T et d'autres organismes de normalisation, notamment l'IETF, l'ISO/CEI JTC 1/SC 6, 25, 27, 31 et 41, élaborer un ensemble de Recommandations définissant des solutions de sécurité complètes pour l'Internet des objets et les services de télécommunication sécurisés.

b) Examiner les Recommandations/normes existantes de l'UIT-T, de l'ISO/CEI et d'autres organismes de normalisation dans le domaine des réseaux domestiques, des réseaux électriques intelligents, de la sécurité des smartphones, de l'Internet des objets et des réseaux de capteurs ubiquitaires pour identifier les services de télécommunication sécurisés.

c) Poursuivre les études afin de définir les aspects relatifs à la sécurité des services de télécommunication et de l'Internet des objets pour un environnement de télécommunication international multifournisseur, et pour les nouveaux services (par exemple les services utilisés pour les villes intelligentes, les réseaux électriques intelligents et les systèmes de contrôle industriel (par exemple les usines intelligentes) qui sont fondés sur les réseaux de télécommunication/TIC).

d) Étudier et recenser les problèmes et menaces de sécurité dans l'Internet des objets et les services de télécommunication sécurisés.

e) Étudier et définir les mécanismes de sécurité pour l'Internet des objets et les services de télécommunication sécurisés.

f) Étudier et définir les mécanismes d'interconnectivité pour l'Internet des objets et les services de télécommunication sécurisés dans un environnement de télécommunication comportant un seul ou plusieurs fournisseurs.

g) Étudier et recenser les problèmes de protection des informations PII et les menaces associées dans l'Internet des objets et les services de télécommunication sécurisés.

h) Étudier et définir les mécanismes de protection et de gestion des informations PII pour l'Internet des objets et les services de télécommunication sécurisés.

i) Étudier et définir des technologies de sécurité basées sur l'intelligence artificielle/l'apprentissage automatique pour l'Internet des objets et les services de télécommunication sécurisés.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 17 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>).

# 4 Relations

Grandes orientations du SMSI:

– C5

Objectifs de développement durable:

– 8 ([Travail décent et croissance économique](http://www.un.org/development/desa/disabilities/envision2030-goal8.html))

– 9 ([Industrie, innovation et infrastructure](http://www.un.org/development/desa/disabilities/envision2030-goal9.html))

– 11 ([Villes et communautés durables](http://www.un.org/development/desa/disabilities/envision2030-goal11.html))

Recommandations:

– Série X et autres Recommandations se rapportant à la sécurité

Questions:

– Questions 1/17, 2/17, 3/17, 4/17, 7/17, 8/17, 10/17, 11/17, 13/17, 14/17 et 15/17 de l'UIT-T

Commissions d'études:

– UIT-R; CE 9, 11, 13, 15, 16 et 20 de l'UIT-T; JCA-IoT et SC&C

Organismes de normalisation:

– Internet Engineering Task Force (IETF); CEI SEG 6 (micro-réseaux électriques), CEI SMB GT3, CEI TC 57 et 65; ISO/CEI JTC 1/SC 6, 25, 27, 31 et 41; Open Mobile Alliance (OMA); Projet de partenariat pour la troisième génération (3GPP); Projet 2 de partenariat pour la troisième génération (3GPP2)

Autres organismes:

– Alliance for Telecommunications Industry Solutions (ATIS); China Communications Standards Association (CCSA); Institut européen des normes de télécommunication (ETSI); GSM Association (GSMA); M2M Alliance; NFC Forum; National Institute of Standards and Technology (NIST); oneM2M; Telecommunication Technology Committee (TTC); Telecommunications Technology Association (TTA); Universal Plug and Play (UPnP)

QUESTION 7/17

Services applicatifs sécurisés

(Suite de la Question 7/17)

# 1 Motifs

Les Recommandations UIT‑T X.1141, X.1142, X.1143, X.1144, X.1145, X.1146 et X.1147 constituent un ensemble de Recommandations sur les jetons de sécurité pour l'authentification/autorisation et les architectures de sécurité pour les messages des services de réseau. Les Recommandations UIT‑T X.1151, X.1152, X.1153, X.1154, X.1155, X.1156, X.1157, X.1158 et X.1159 indiquent les lignes directrices applicables à un protocole d'authentification sûre fondée sur un mot de passe avec échange de clés et divers services de tiers de confiance (TTP). Les Recommandations UIT‑T X.1161, X.1162, X.1163 et X.1164 indiquent un cadre complet et des mécanismes pour la sécurité des services P2P. Il faut poursuivre les efforts pour mettre à jour et améliorer ces Recommandations relatives à la sécurité afin de répondre aux besoins des nouvelles technologies et des nouveaux services.

Le secteur des télécommunications connaît une croissance exponentielle des services de tiers de confiance (TTP). La sécurité des services applicatifs basés sur les télécommunications (par exemple services de réseaux sociaux, services P2P et services TTP) est indispensable pour le développement futur du secteur. Les protocoles applicatifs sécurisés jouent un rôle très important dans la fourniture de services applicatifs sécurisés. La normalisation de solutions de sécurité complètes optimales est essentielle pour les entreprises et les opérateurs de réseau qui travaillent dans un environnement international multifournisseur. De plus, il faut aussi étudier et définir d'autres types de plates-formes et de services applicatifs sécurisés comme les services d'horodatage, les services notariaux sécurisés, les services sécurisés des technologies financières (systèmes bancaires ouverts, prêts entre homologues, envois de fonds, portefeuilles mobiles, assurances), les services OTT sécurisés et les jumeaux numériques; l'utilisation d'assertions de sécurité au lieu d'utiliser des certificats dans les protocoles fondés sur l'infrastructure PKI et les services applicatifs PKI, etc. Les technologies de sécurité comme l'assertion de sécurité et l'assertion de contrôle d'accès deviennent très importantes dans les réseaux de communication.

À mesure que des services applicatifs apparaissent dans le domaine des télécommunications/TIC, deux nouveaux horizons s'ouvrent et doivent être explorés: les applications produisent et traitent de plus en plus de données et il est désormais nécessaire de s'appuyer sur l'intelligence artificielle. Il faut élargir les services applicatifs sécurisés afin de réaliser une étude de marché approfondie, dans l'optique d'examiner tous les aspects opérationnels et techniques de la protection des données, qui s'appuie sur les travaux existants en matière de services d'analyse de données.

S'agissant de l'intelligence artificielle, les fournisseurs de services sont confrontés à plusieurs défis, en particulier la sélection et l'intégration de dizaines voire de centaines de composants d'IA, qu'ils soient *open source* ou tirés du secteur privé. Les fournisseurs doivent assembler ces composants dans des solutions diverses reposant sur l'IA (applications intégrées, plates-formes plus génériques, plate-forme en tant que service, etc.), au sein de différentes infrastructures (réseau local, nuage privé, nuage hybride, nuage public). Comme cela a été le cas avec l'apparition des mégadonnées, de nouveaux problèmes se posent quant à l'interopérabilité en termes de sécurité, mais aussi pour ce qui est de garantir la confidentialité, l'intégrité et la disponibilité des données, qu'il s'agisse des données d'apprentissage alimentant l'IA ou des données générées par l'IA. Tout cela implique de nouvelles vulnérabilités de l'intelligence artificielle et nécessite des études et des développements. Ces efforts peuvent également s'appuyer sur les travaux existants en matière de services d'analyse de données.

Recommandations et Suppléments relevant de la présente Question au 7 janvier 2022: Recommandations X.1141, X.1142, X.1143, X.1144, X.1145, X.1146, X.1147, X.1148, X.1149, X.1151, X.1152, X.1153, X.1154, X.1155, X.1156, X.1157, X.1158, X.1159, X.1161, X.1162, X.1163, X.1164, X.1450, X.1451, X.1452, X.1470 et Suppléments X.Suppl.17, X.Suppl.21 et X.Suppl.22.

Textes en cours d'élaboration au 7 janvier 2022: X.1144rev, X.guide-cdd, X.rdda, X.saf-dfs, X.scpa, X.sec-grp-mov, X.sg-dtn, X,sles, X.smdtsc, X.smsrc, X.vide, X.websec-7 et TR.cta.

# 2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

a) Comment identifier et traiter les menaces qui pèsent sur les services applicatifs sécurisés?

b) Quelles technologies de sécurité peuvent être utilisées pour la fourniture de services applicatifs sécurisés?

c) Comment assurer et maintenir une interconnectivité sécurisée entre les services applicatifs?

d) Quels protocoles ou techniques de sécurité sont nécessaires pour les services applicatifs sécurisés?

e) Quels protocoles ou techniques de sécurité sont nécessaires pour les nouveaux services applicatifs sécurisés, y compris les plates-formes de services, les services des technologies financières et les services OTT?

f) Quelles sont les solutions de sécurité globales pour les services applicatifs sécurisés et pour leurs applications?

g) Comment définir une stratégie pour la protection des données opérationnelles et techniques des services applicatifs?

h) Comment définir une stratégie pour remédier aux vulnérabilités de l'intelligence artificielle?

# 3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

a) En collaboration avec d'autres Commissions d'études de l'UIT‑T et d'autres organismes de normalisation, notamment l'ISO/CEI JTC 1/SC 27, élaborer un ensemble complet de Recommandations définissant des solutions de sécurité complètes pour les services applicatifs sécurisés.

b) Examiner les Recommandations/normes existantes de l'UIT‑T et de l'ISO/CEI dans le domaine des services applicatifs sécurisés.

c) Mener des études complémentaires pour définir les aspects de sécurité des services applicatifs sécurisés existants ou nouveaux, y compris les services des technologies financières et les services OTT.

d) Étudier et recenser les problèmes et menaces de sécurité dans les services applicatifs sécurisés.

e) Étudier et définir les mécanismes de sécurité pour les services applicatifs sécurisés.

f) Étudier et élaborer des stratégies et des Recommandations concernant les aspects opérationnels et techniques de la protection des données pour les services applicatifs.

g) Étudier et élaborer des stratégies et des Recommandations pour remédier aux vulnérabilités de l'intelligence artificielle.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 17 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>).

# 4 Relations

Grandes orientations du SMSI:

– C5

Objectifs de développement durable:

– 8 ([Travail décent et croissance économique](http://www.un.org/development/desa/disabilities/envision2030-goal8.html))

– 9 ([Industrie, innovation et infrastructure](http://www.un.org/development/desa/disabilities/envision2030-goal9.html))

– 11 ([Villes et communautés durables](http://www.un.org/development/desa/disabilities/envision2030-goal11.html))

Recommandations:

– Série X.800 et autres Recommandations se rapportant à la sécurité

Questions:

– Questions 1/17, 2/17, 3/17, 4/17, 6/17, 8/17, 10/17, 11/17, 13/17, 14/17, 15/17, et 7/13 de l'UIT-T

Commissions d'études:

– CE 2, 9, 11, 13, 16 et 20 de l'UIT-T

Organismes de normalisation:

– Internet Engineering Task Force (IETF); Institut européen des normes de télécommunication (ETSI); GSM Association (GSMA); ISO/CEI JTC 1/SC 27, ISO/CEI JTC 1/SC 42, ISO/TC 68, ISO/TC 307; Kantara Initiative; Organization for the Advancement of Structured Information Standards (OASIS); Open Mobile Alliance (OMA); World Wide Web Consortium (W3C)

Autres organismes:

– Conseil de l'Europe; Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA); Fast Identity Online (FIDO) Alliance; International Multilateral Partnership Against Cyber Threats (IMPACT)

QUESTION 8/17

Sécurité de l'informatique en nuage et de l'infrastructure des mégadonnées

(Suite de la Question 8/17)

# 1 Motifs

L'informatique dématérialisée, ou informatique en nuage, est un modèle permettant d'offrir à un utilisateur de services un accès ubiquitaire, pratique, à la demande et via le réseau à un ensemble mutualisé de ressources informatiques configurables (par exemple réseaux, serveurs, mémoires, applications et services), qui peuvent être rapidement mobilisées et mises à disposition moyennant un minimum de gestion ou d'interaction avec le fournisseur de services. Le modèle de l'informatique en nuage comporte cinq caractéristiques essentielles (à la demande, accès universel via le réseau, mutualisation des ressources, élasticité rapide, libre-service avec facturation à l'utilisation), cinq catégories de services (à savoir logiciel en tant que service (SaaS, *software as a service*), communication en tant que service (CaaS, *communication as a service*), plate‑forme en tant que service (PaaS, *platform as a service*), infrastructure en tant que service (IaaS, *infrastructure as a service*) et réseau en tant que service (NaaS, *network as a service*)) ainsi que différents modèles de déploiement (public, privé, hybride …) et permet un élargissement souple des types de fourniture des services (au niveau central, au niveau régional, en périphérie). L'informatique en nuage est devenue le support privilégié pour la découverte, l'externalisation, la composition et la réutilisation des services dans des flux de travail, des applications et des applications fondées sur les communications, de sorte que l'exigence de sécurité revêt une importance accrue.

L'informatique en nuage devrait offrir divers avantages tels que la fourniture de ressources souple et dynamique et une simplification ainsi qu'une automatisation de l'administration des infrastructures informatiques. La virtualisation permet de partager une quantité quasi illimitée de ressources et permet d'améliorer l'évolutivité et de réduire massivement les coûts liés à la gestion des infrastructures. L'informatique en périphérie permet la distribution des capacités de nuage jusqu'à la périphérie du réseau. Cela donne lieu à la mise en œuvre de services en nuage avec des taux de latence faibles et déterministes. Toutefois, les systèmes ouverts, les ressources partagées et l'interfonctionnement inhérent de l'informatique en nuage et de l'informatique en périphérie soulèvent bon nombre de problèmes de sécurité, ce qui constitue peut-être l'obstacle le plus important à leur adoption. Le passage à l'informatique en nuage signifie que les systèmes informatiques internes sécurisés classiques seront supplantés par des infrastructures ouvertes, non sécurisées et "mises en nuage", d'où la nécessité de "repenser" radicalement le concept de sécurité.

L'informatique en nuage a été considérée pendant plusieurs années comme étant centrée sur les services informatiques et contrôlée par les acteurs de l'Internet. Toutefois les acteurs des télécommunications ont un rôle important à jouer sur le marché et dans l'écosystème émergents de l'informatique en nuage. Les services en nuage étant fournis par l'intermédiaire des réseaux de télécommunication, les acteurs des télécommunications devraient assurer un niveau de garantie élevé. Une protection de la sécurité efficace et offrant la souplesse voulue sera un élément déterminant du marché et de l'écosystème de l'informatique en nuage dans leur ensemble, en particulier dans la mesure où l'informatique en périphérie permet une répartition plus locale des ressources en nuage. Cela complique les relations entre les mises en œuvre respectives du nuage en périphérie, au niveau régional et au niveau central.

En outre, la souplesse d'utilisation de ressources précieuses dans les environnements informatiques en nuage permettra de fournir de nouveaux services de sécurité que les dispositifs de protection actuels ne peuvent assurer (par exemple les services de lutte contre les logiciels malveillants en tant que service en nuage).

Les mégadonnées sont considérées comme l'ensemble de technologies, d'outils, de données et d'analyses qui sont utilisés pour traiter de grands volumes de données. En outre, à mesure que les données augmentent de façon exponentielle et qu'elles deviennent un élément clé des réseaux de télécommunication/TIC, des volumes importants de données sont analysés grâce à l'informatique en nuage pour mettre en lumière les configurations et les relations qui, sinon, resteraient cachées. Les processus centraux relatifs aux mégadonnées, tels que la collecte, le stockage, l'analyse, la gestion et la visualisation des données sont basés sur l'informatique en nuage. Les technologies classiques (par exemple les mégadonnées en tant que service) ne permettent pas de transférer et d'analyser les mégadonnées aussi rapidement. En conséquence, il faut examiner quels types de mesures de sécurité l'informatique en nuage pourra assurer à brève échéance. Les Recommandations UIT‑T X.1601, X.1602 et X.1631 constituent un ensemble de Recommandations relatives aux services de sécurité pour l'aperçu général, l'architecture et le cadre de sécurité de l'informatique en nuage, la sécurité en nuage transcouche et la sécurité propre aux services de réseau. À l'heure actuelle, il est essentiel de sécuriser les services (services critiques vocaux, multimédias, d'identité, assurance des informations, services d'identité et de données et services d'urgence) rendus possibles par l'informatique en nuage. La présente Question a pour objet d'élaborer de nouvelles Recommandations, à partir du rapport technique (Partie 5) du Groupe spécialisé sur l'informatique dématérialisée, sur les thèmes suivants:

– bonnes pratiques et lignes directrices à élaborer pour donner des orientations sur la manière d'assurer la sécurité dans un environnement utilisant l'informatique en nuage;

– clarification des responsabilités et définition des exigences de sécurité ainsi que des menaces qui pèsent sur la sécurité pour les principaux acteurs et rôles correspondants dans l'écosystème de l'informatique en nuage;

– architecture de sécurité fondée sur l'architecture de référence décrite au titre de la Question 18/13;

– gestion de la sécurité et technologies d'audit pour la gestion de la confiance.

Les responsables de la Question 8/17 collaboreront avec les responsables des Questions connexes, par exemple les Questions 2/17, 3/17, 4/17, 7/17, 10/17 et 11/17, en vue d'élaborer des Recommandations relatives à la sécurité de l'informatique en nuage.

Recommandations et Rapports techniques relevant de la présente Question au 7 janvier 2022: X.1601, X.1602, X.1603, X.1604, X.1605, X.1606, X.1631, X.1641, X.1642, X.1643, X.1750, X.1751, X.1752 et Rapport technique TR.XAASL.

Textes en cours d'élaboration au 7 janvier 2022: X.BaaS-sec, X.gecds, X.nssa-cc, [X.sa-ec](https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16951), X.sgcnp, X.sgdc, X.sgmc et X.sr-cphr.

# 2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

a) Quelles nouvelles Recommandations ou autres types de documents convient-il d'élaborer à l'intention des principaux acteurs – fournisseurs et utilisateurs de services et partenaires – ainsi que des autres principaux acteurs concernés, pour promouvoir la sécurité de tout l'écosystème de l'informatique en nuage, y compris la sécurité de l'informatique en nuage, la sécurité de l'informatique en périphérie, la sécurité de l'interfonctionnement, etc.?

b) Quelles nouvelles Recommandations convient-il d'élaborer concernant l'architecture de la sécurité et l'organisation des fonctionnalités de la sécurité conformément à l'architecture de référence?

c) Quelles nouvelles Recommandations convient-il d'élaborer concernant les mécanismes de garantie, les technologies d'audit et l'évaluation des risques associés pour instaurer la confiance entre les différents acteurs?

d) Quelles nouvelles Recommandations convient-il d'élaborer concernant les solutions, les bonnes pratiques ou les lignes directrices relatives à la sécurité des infrastructures et des plates-formes de mégadonnées?

e) Quelle collaboration faut-il établir avec d'autres Questions, commissions d'études et organismes de normalisation pour éviter autant que possible toute répétition des tâches?

f) Comment la sécurité en tant que service doit-elle être mise au point pour protéger les systèmes de télécommunication/TIC?

# 3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

a) Élaborer des Recommandations ou d'autres types de documents pour promouvoir la sécurité de l'informatique en nuage.

b) Élaborer des Recommandations pour définir les menaces et les exigences de sécurité pour les services liés à l'informatique en nuage sur la base des exigences générales définies par la Commission d'études 13 de l'UIT‑T en matière d'informatique en nuage.

c) Élaborer des Recommandations pour définir l'architecture de sécurité et organiser les fonctions de sécurité sur la base de l'architecture de référence définie par la Commission d'études 13 de l'UIT‑T.

d) Élaborer des Recommandations pour définir une architecture et une mise en œuvre de la sécurité efficaces, souples et élastiques pour les systèmes informatiques en nuage.

e) Élaborer des Recommandations pour déterminer des mécanismes de garantie, des technologies d'audit et une évaluation des risques, l'objectif étant d'établir des relations de confiance dans l'écosystème de l'informatique en nuage.

f) Étudier et élaborer des Recommandations concernant la sécurité des infrastructures et des plates-formes de mégadonnées, conformément à l'architecture de référence définie par la Commission d'études 13 de l'UIT-T.

g) Assumer la responsabilité de toutes les activités liées à la sécurité de l'informatique en nuage ainsi des infrastructures et des plates-formes de mégadonnées au sein de la Commission d'études 17.

h) Représenter la Commission d'études 17, pour ce qui est des travaux relatifs à la sécurité de l'informatique en nuage, au sein de l'activité conjointe de coordination sur l'informatique en nuage.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 17 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>).

# 4 Relations

Grandes orientations du SMSI:

– C5

Objectifs de développement durable:

– 8 ([Travail décent et croissance économique](http://www.un.org/development/desa/disabilities/envision2030-goal8.html))

– 9 ([Industrie, innovation et infrastructure](http://www.un.org/development/desa/disabilities/envision2030-goal9.html))

– 11 ([Villes et communautés durables](http://www.un.org/development/desa/disabilities/envision2030-goal11.html))

Recommandations:

– Recommandations de la série Y relatives à l'informatique en nuage

Questions:

– Questions 1/17, 2/17, 3/17, 4/17, 7/17, 10/17, 11/17 et 15/17 de l'UIT‑T

Commissions d'études:

– CE 2, 13, 16 et 20 de l'UIT‑T

Organismes de normalisation:

– Internet Engineering Task Force (IETF); ISO/CEI JTC 1/SC 27 et SC 38; Organization for the Advancement of Structured Information Standards (OASIS) et autres organismes concernés identifiés

Autres organismes:

– Cloud Security Alliance (CSA); Distributed Management Task Force (DMTF)

QUESTION 10/17

Architecture et mécanismes de gestion des identités et de télébiométrie

(Suite de la Question 10/17)

# 1 Motifs

La biométrie est de plus en plus répandue dans les applications utilisées pour la vérification d'identité (mais pas exclusivement), notamment dans les domaines du commerce électronique, de la télémédecine et de la cybersanté. Les systèmes biométriques posent divers problèmes liés à la protection des données opérationnelles et techniques, à la fiabilité et à la sécurité des données biométriques pour les applications de biosûreté et de biosécurité.

L'authentification biométrique côté serveur se complique et pose de multiples problèmes lorsqu'elle est adoptée dans un environnement de réseau ouvert. Les applications de télécommunication (telles que la télébiométrie) utilisant les terminaux mobiles et les services Internet nécessitent des méthodes d'authentification pour garantir une utilisation très sécurisée et conviviale. Il est nécessaire de spécifier des exigences pour que les données télébiométriques soient utilisées de manière sûre et sécurisée et pour renforcer la protection des données opérationnelles et techniques.

La gestion des identités (IdM) est la gestion du cycle de vie et de l'utilisation (création, tenue à jour, utilisation et révocation) des justificatifs, identificateurs, attributs et profils au moyen desquels les entités (par exemple fournisseurs de services, utilisateurs finals, organisations, dispositifs de réseau, applications et services) sont connues avec un certain degré de confiance. Suivant le contexte, de multiples identités peuvent exister pour une même entité en des endroits multiples et pour répondre à différentes exigences de sécurité. Suivant le modèle d'identité, le contrôle des identités peut être centralisé, décentralisé ou une combinaison des deux. Dans les réseaux publics, l'IdM permet un échange sécurisé d'informations entre entités autorisées, sur la base de la confirmation des identités émanant de plusieurs fournisseurs de services, à travers des systèmes répartis. L'échange peut également se baser sur plusieurs environnements de service tels que l'informatique en nuage et la 5G. L'IdM permet également de renforcer la protection des informations privées et, lorsqu'elle s'appuie sur le modèle de confiance, de garantir que seules les informations autorisées sont diffusées.

L'IdM est un élément essentiel des réseaux, services et produits de télécommunication/TIC, car elle permet d'établir et de maintenir des communications fiables. Elle permet non seulement l'authentification de l'identité d'une entité, mais aussi l'autorisation des accès sur la base de privilèges, la modification des privilèges lorsqu'une entité change de rôle, la délégation et d'autres services basés sur l'identité.

L'IdM est un élément critique pour la gestion de la sécurité de réseau, car elle permet de mieux répondre aux attentes des utilisateurs finals en termes d'accès nomade à la demande aux réseaux et aux services. Conjointement avec d'autres mécanismes de défense, l'IdM contribue à prévenir les fraudes et les vols d'identité et ainsi à augmenter la confiance des utilisateurs dans la sécurité et la fiabilité des transactions. Étant donné que l'IdM est basée sur la réciprocité, le renforcement de la confiance concerne aussi bien l'utilisateur final que le fournisseur de services.

Il existera différentes spécifications et solutions IdM nationales ou régionales, qui continueront à évoluer. Il est important de jeter les bases qui permettront d'harmoniser les solutions. Outre l'étude de la télébiométrie, la présente Question vise à définir la vision ainsi qu'à coordonner et à organiser toutes les activités relatives à l'IdM au sein de l'UIT-T. Une méthode descendante relative à l'IdM sera utilisée en collaboration avec d'autres Commissions d'études et d'autres organismes de normalisation. Il est admis que certains aspects de l'IdM (protocoles, exigences, identifiants de dispositif de réseau, etc.) relèveront d'autres Questions.

Recommandations et Suppléments relevant de la présente Question au 7 janvier 2022: X.1080.0, X.1080.1, X.1080.2, X.1081, X.1082, X.1083, X.1084, X.1085, X.1086, X.1087, X.1088, X.1089, X.1090, X.1091, X.1092, X.1093, X.1094, X.1250, X.1251, X.1252, X.1253, X.1254, X.1255, X.1256, X.1257, X.1258, X.1261 (avec la CE 2), X.1275, X.1276, X.1277, X.1278, X.1279 et Suppléments X.Suppl.7 et X.Suppl.35.

Textes en cours d'élaboration au 7 janvier 2022: X.1250rev, X.gpwd, X.oob-sa, X.pet\_auth, X.srdidm et X.tec-idms.

# 2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

a) Comment améliorer encore ou réviser les Recommandations actuelles pour qu'elles soient largement déployées et utilisées?

b) Quelles sont les exigences de l'authentification biométrique dans un réseau comportant de nombreuses fonctionnalités?

c) Comment évaluer les contre‑mesures de sécurité pour des applications particulières de télébiométrie?

d) Comment définir les systèmes et opérations biométriques pour qu'ils soient conformes aux exigences de sécurité de n'importe quelle application de télébiométrie, y compris les services informatiques en nuage?

e) Comment peut-on améliorer l'identification et l'authentification des utilisateurs en termes de sécurité et de sûreté en utilisant des modèles télébiométriques interopérables?

f) Quels mécanismes faut-il prendre en charge pour garantir la sûreté et la sécurité de manipulation des données biométriques dans les applications de télébiométrie tant existantes qu'émergentes, par exemple la cybersanté, la télémédecine, le commerce électronique, les services bancaires en ligne ou la vidéosurveillance?

g) Comment définir les systèmes et opérations biométriques pour qu'ils soient conformes aux exigences fonctionnelles d'authentification d'entité pour les animaux de compagnie au moyen de la télébiométrie?

h) Quels sont les concepts fonctionnels d'une infrastructure commune de gestion des identités (IdM)?

i) Comment définir un modèle IdM approprié qui soit indépendant des technologies de réseau, qui soit centré sur l'utilisateur, qui prenne en charge la gestion en nuage des identités et les modèles d'identité décentralisés et qui permette un échange sécurisé des informations IdM entre les entités concernées (par exemple utilisateurs, parties utilisatrices et fournisseurs d'identité) sur la base des politiques de consentement et des politiques connexes?

j) Quelles sont les composantes d'un cadre générique et les exigences concernant la gestion des identités?

k) Quelles sont les exigences particulières de la gestion des identités pour les fournisseurs de service?

l) Quelles sont les exigences, les capacités et les stratégies possibles pour parvenir à une interopérabilité entre différents systèmes IdM (par exemple garantie d'identité, interfonctionnement)?

m) Quels sont les aspects à prendre en compte concernant la gestion des identités dans le cadre des technologies de registres distribués, y compris les porte-monnaie numériques, les identificateurs décentralisés et les justificatifs vérifiables?

n) Quels sont les mécanismes envisageables en matière d'interopérabilité des systèmes IdM, par exemple l'identification et la définition de profils applicables, pour réduire au minimum les problèmes liés à l'interopérabilité?

o) Quelles sont les exigences et les mécanismes concernant la protection et la divulgation des informations d'identification personnelle (PII)?

p) Comment une entité peut-elle contrôler ses relations lorsqu'elle est engagée dans des relations et interactions fondées sur des identités?

q) Quelles sont les exigences applicables à la protection des systèmes IdM contre les cyberattaques?

r) Quelles capacités IdM peuvent être utilisées contre les cyberattaques?

s) Comment doit-on intégrer l'IdM avec les technologies de sécurité avancées?

t) Comment procéder à une authentification sans utiliser de secrets partagés?

u) L'authentification basée sur l'infrastructure PKI peut-elle être effectuée de manière interopérable et sécurisée?

v) La biométrie peut-elle être utilisée dans le cadre de l'authentification forte et de la couche de confiance pour garantir la fiabilité des interactions dans un réseau?

w) Quelles sont les exigences propres aux systèmes de gestion des identités basés sur les consommateurs en termes de vérification des identités et de récupération des comptes sans mot de passe?

x) Comment la confiance et les relations peuvent-elles être exploitées pour améliorer la récupération des comptes, la sécurité et l'expérience des utilisateurs lorsqu'il est fait appel à des parties utilisatrices?

# 3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

a) Améliorer et réviser les Recommandations actuelles sur l'authentification télébiométrique.

b) Examiner les similitudes et les différences entre les Recommandations UIT-T et les normes de l'ISO/CEI existantes relatives à la télébiométrie.

c) Étudier et définir les exigences et lignes directrices relatives à la sécurité de n'importe quelle application de télébiométrie sur la base des architectures et des cadres tels que ceux définis au titre de la Question 2/17.

d) Étudier et définir les exigences pour évaluer les méthodes de sécurité et de protection des données opérationnelles et techniques pour n'importe quelle application de télébiométrie.

e) Étudier et définir les exigences des applications télébiométriques dans un réseau comportant de nombreuses fonctionnalités.

f) Étudier et définir les exigences et cadres intégrés relatifs aux applications télébiométriques pour les environnements de l'informatique en nuage et du stockage des données.

g) Étudier et définir les exigences d'authentification télébiométrique pour un cadre d'identité sécurisé.

h) Étudier et définir les exigences des protocoles génériques appropriés concernant la sûreté, la sécurité, la protection des données opérationnelles et techniques et l'accord "pour la manipulation de données biométriques" dans n'importe quelle application de télébiométrie, par exemple la cybersanté, la télémédecine, le commerce électronique, les services bancaires en ligne, le paiement en ligne ou la vidéosurveillance.

i) Étudier et définir des protocoles biologie-machine (B2M) de transmission de métriques biologiques qui soient compatibles avec les protocoles machine-machine (M2M).

j) Étudier et définir des applications télébiométriques utilisant des bio-signaux pour des applications d'authentification, d'identification, de suivi de l'état de santé, etc.

k) Étudier et élaborer des services d'authentification d'entité pour les animaux de compagnie, sur la base de la télébiométrie.

l) Spécifier un cadre IdM qui prenne en charge un modèle de découverte, de politique et de confiance, l'authentification et l'autorisation, les assertions et la gestion du cycle de vie des justificatifs d'identité nécessaires pour l'IdM.

m) Définir les concepts fonctionnels de l'architecture IdM afin d'assurer un relais IdM entre réseaux et entre systèmes IdM compte tenu des technologies de sécurité avancées.

n) Définir des exigences (et proposer des mécanismes) concernant la garantie d'identité et la mise en correspondance/l'interfonctionnement de différentes méthodes de garantie d'identité qui pourraient être adoptées dans divers réseaux. Dans ce contexte, la garantie d'identité recouvre les profils d'identité et la réputation.

o) Définir des interfaces pour l'interopérabilité des systèmes IdM.

p) Définir des exigences (et proposer des mécanismes) concernant la protection et la divulgation des informations d'identification personnelle (PII).

q) Définir des exigences (et proposer des mécanismes) concernant la protection des systèmes IdM, y compris l'utilisation par les fournisseurs de service de capacités IdM pour se coordonner et échanger des informations concernant les cyberattaques.

r) Mettre à jour et coordonner une liste ouverte de termes et définitions concernant l'IdM.

s) Étudier et définir les risques et menaces de sécurité liés à l'IdM.

t) Étudier et élaborer des systèmes de gestion décentralisée des identités pour permettre aux utilisateurs de contrôler leurs identités.

u) Faire en sorte qu'une fédération des systèmes de gestion des identités fiables soit possible à travers les systèmes, les services, les dispositifs, l'Internet des objets et les applications.

v) Faire en sorte que les systèmes de gestion des identités puissent assurer une gestion des identités en tant que service pour les agents en nuage, les réseaux 5G et les dispositifs mobiles.

w) Définir les exigences et proposer des mécanismes concernant la garantie d'identité, l'authentification et la fédération. Établir des critères pour la mise en correspondance/l'interfonctionnement de différentes méthodes de garantie d'identité qui pourraient être adoptées dans divers réseaux. Dans ce contexte, la garantie d'identité recouvre les profils d'identité et la réputation.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 17 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>).

# 4 Relations

Grandes orientations du SMSI:

– C5

Objectifs de développement durable:

– 8 ([Travail décent et croissance économique](http://www.un.org/development/desa/disabilities/envision2030-goal8.html))

– 9 ([Industrie, innovation et infrastructure](http://www.un.org/development/desa/disabilities/envision2030-goal9.html))

Recommandations:

– Séries X et Y

– Recommandations X.200, X.273, X.274, X.509, X.680, X.805 et X.1051

Questions:

– Questions 1/17, 2/17, 3/17, 4/17, 6/17, 7/17, 8/17, 11/17, 15/17, 7/13 et 14/15 de l'UIT‑T

Commissions d'études:

– CE 1 et 2/2 de l'UIT-D; CE 7 de l'UIT-R; CE 2, 5, 9, 11, 13, 15, 16 et 20 de l'UIT-T

Organismes de normalisation:

– CEI/TC 25, CEI/TC 25/JWG 1; Institute of Electrical and Electronics Engineers (IEEE); Internet Engineering Task Force (IETF); ISO/CEI JTC 1/SC 6, 17, 27 et 37; ISO/TC 12, 68, 215 et 307; ISO/TC 12/JWG 20; ETSI; OASIS; Kantara Initiative; 3GPP; 3GPP2

Autres organismes:

– Bureau international des poids et mesures (BIPM); Commission internationale des unités et mesures radiologiques (ICRU); Fast Identity Online (FIDO) Alliance; DID Alliance; Bureau international du travail (BIT); Organisation mondiale de la santé (OMS)

QUESTION 11/17

Technologies génériques (notamment: annuaire, infrastructure de clé publique (PKI), langages formels et identificateurs d'objets) utilisées
pour les applications sécurisées

(Suite de la Question 11/17)

# 1 Motifs

La présente Question vise à encourager la poursuite du développement de diverses technologies génériques qui sont largement utilisées pour les applications sécurisées, à savoir:

– Services d'annuaire (série X.500)

– Infrastructures de clés publiques (PKI – X.509)

– Communications sécurisées (X.510)

– Infrastructure de gestion des privilèges (PMI – X.509)

– Syntaxe abstraite numéro un (ASN.1)

– dentificateurs d'objet et leurs autorités d'enregistrement

– Notation de test et de commande de test version 3 (TTCN-3)

– Maintenance des langages formels:

• Langage de description et de spécification (SDL)

• Conception d'un profil de langage de modélisation unifié (UML)

• Diagrammes de séquences de messages (MSC)

• Notation des besoins de l'utilisateur (URN)

• CHILL, le langage de programmation de l'UIT-T

– Tenue à jour des Recommandations OSI et ODP

## 1.1 Motifs pour les travaux sur les annuaires et les infrastructures PKI et PMI

La série X.500 de Recommandations UIT-T a une grande incidence dans les entreprises. Ces Recommandations, sur lesquelles reposent en grande partie des technologies largement déployées telles que l'infrastructure de clé publique (PKI) et le protocole simple d'accès à l'annuaire (LDAP), sont utilisées dans de nombreux domaines, par exemple financier, médical et juridique. Lorsque des services d'annuaire présentant une grande sécurité sont nécessaires, par exemple dans le domaine militaire, la série X.500 est la seule solution.

La série X.500 définit des mécanismes détaillés de contrôle d'accès et de protection de la confidentialité des données. Il s'agit d'une spécification ouverte qui peut être adaptée à de nombreuses applications différentes. Elle peut être étendue afin de répondre aux exigences futures. Le protocole LDAP largement utilisé est fondé sur le modèle d'annuaire X.500. La Recommandation UIT‑T X.500 comporte des fonctionnalités permettant un interfonctionnement avec le protocole LDAP. La gestion des identités (IdM) repose en grande partie sur les solutions d'annuaire X.500 et LDAP.

La Recommandation UIT‑T X.509 est importante. Les certificats de clés publiques sont largement utilisés.

Outre le rôle majeur qu'ils jouent dans le commerce en ligne, dans les services bancaires en ligne et dans la cybersanté, ils sont désormais également utilisés dans d'autres domaines s'appuyant sur de grands réseaux, avec des communications de machine à machine et des entités contraintes, par exemple l'Internet des objets et les réseaux électriques intelligents.

Les certificats de clé publique sont également utilisés pour plusieurs spécifications de l'IETF, par exemple la sécurité dans la couche transport (TLS).

Les certificats d'attribut constituent une méthode sûre pour transmettre les privilèges qui sont importants pour le contrôle d'accès. Les spécifications SAML OASIS sont fondées sur les certificats d'attribut X.509. Les certificats d'attribut sont également utilisés dans les systèmes d'alimentation électrique. Ils sont utiles en particulier lorsque des privilèges sont assignés par des autorités autres que celles qui ont délivré les certificats de clé publique.

En collaboration avec d'autres groupes, il faut actualiser la Recommandation UIT‑T X.509 afin de tenir compte et de tirer parti des expériences acquises dans le domaine de l'infrastructure de clés publiques (PKI) et dans celui de l'infrastructure de gestion des privilèges (PMI). Des améliorations doivent être apportées à la Recommandation UIT‑T X.509 afin de tenir compte des nouvelles exigences relatives aux communications machine-machine, à la sécurité des réseaux électriques intelligents, à la sécurité de l'Internet des objets, aux algorithmes à l'épreuve des attaques quantiques et aux technologies des registres distribués. Un mécanisme PKI décentralisé basé sur la chaîne de blocs est en cours d'élaboration.

Recommandations relevant de la présente Question au 7 janvier 2022: E.104 et E.115 (conjointement avec la CE 2), F.500, F.510, F.511, F.515, X.500, X.501, X.509, X.510, X.511, X.518, X.519, X.520, X.521, X.525, X.530 et X.1341.

Textes en cours d'élaboration au 7 janvier 2022: Amendement 1 à la Recommandation X.510 et X.pki-em.

## 1.2 Motifs pour les travaux sur l'ASN.1

De nouvelles Recommandations seront élaborées selon qu'il sera nécessaire pour tenir compte des progrès technologiques et des besoins supplémentaires des utilisateurs concernant la notation ASN.1 et ses règles de codage.

L'ASN.1 s'est révélée être la notation de prédilection pour de nombreux groupes de normalisation de l'UIT-T, dont un grand nombre continue de demander que des corrections soient apportées pour résoudre des problèmes d'ambiguïté ou de manque de clarté.

Les autres Commissions d'études, les organismes de normalisation externes et les pays demandent régulièrement des conseils et une assistance sur la notation ASN.1.

Recommandations relevant de la présente Question au 7 janvier 2022: X.680, X.681, X.682, X.683, X.690, X.691, X.692, X.693, X.694, X.695, X.696, X.697, X.891, X.892, X.893 et X.894.

Textes en cours d'élaboration au 7 janvier 2022: Aucun.

## 1.3 Motifs pour les travaux sur les identificateurs d'objet et sur leurs autorités d'enregistrement

Les identificateurs d'objet (OID) se sont avérés être un espace de noms très apprécié, basé essentiellement sur une structure arborescente d'autorités d'enregistrement hiérarchiques identifiées par un entier. L'extension récente de cet espace de noms aux identificateurs d'objet internationaux permettant d'identifier les arcs par des étiquettes Unicode est également appréciée pour diverses applications, et une nouvelle extension sera probablement nécessaire, pour de nouvelles attributions.

Les autres Commissions d'études, les organismes de normalisation externes et les pays demandent régulièrement des conseils et une assistance sur la gestion de l'espace de noms des identificateurs d'objet. Les besoins d'aide et de conseils devraient augmenter avec la mise en place des identificateurs d'objet internationaux et l'utilisation croissante d'autorités d'enregistrement nationales par les pays en développement. Il est donc nécessaire de poursuivre le "Projet OID" de l'UIT‑T placé sous la responsabilité d'un chef de projet afin de répondre à ces besoins.

Toute utilisation innovante des identificateurs d'objet doit être mise au point conjointement avec la Commission d'études 2 de l'UIT‑T.

Recommandations et documents techniques relevant de la présente Question au 7 janvier 2022: X.660, X.662, X.665, X.666, X.667, X.668, X.669, X.670, X.671, X.672, X.674, X.675, X.676, X.677 et document technique XSTP-OID-ORS.

Textes en cours d'élaboration au 7 janvier 2022: révision de la Recommandation X.672.

## 1.4 Motifs pour les travaux sur la notation TTCN-3

La notation de test et de commande de test version 3 (TTCN-3) permet de spécifier des tests de fonctionnalité et d'interopérabilité de systèmes et de concevoir des suites de tests génériques. La notation TTCN-3 est utilisée dans les Recommandations UIT-T relatives aux tests élaborées par les Commissions d'études compétentes de l'UIT-T, en particulier la CE 11, en sa qualité de commission d'études directrice pour les spécifications de test ainsi que pour les tests de conformité et d'interopérabilité. L'UIT-T produit un grand nombre de Recommandations. Pour assurer l'interopérabilité, il est essentiel que les mises en œuvre de ces Recommandations soient conformes aux Recommandations.

Recommandations relevant de la présente Question au 7 janvier 2022: X.292, Z.161, Z.161.1, Z.161.2, Z.161.3, Z.161.4, Z.161.5, X.161.6, Z.161.7, Z.162, Z.163, Z.164, Z.165, Z.165.1, Z.166, Z.167, Z.168, Z.169, Z.170 et Z.171.

Textes en cours d'élaboration au 7 janvier 2022: Aucun.

## 1.5 Motifs pour les travaux sur la maintenance des langages formels

Aucune évolution n'est prévue concernant les langages formels suivants:

– Langage de description et de spécification (SDL)

– Profil de langage de modélisation unifié (UML)

– Diagrammes de séquences de messages (MSC)

– Notation des besoins de l'utilisateur (URN)

– CHILL, le langage de programmation de l'UIT-T

Toutefois, il est nécessaire d'assurer la maintenance de ces langages en permanence.

Recommandations, Suppléments et Guides de mise en œuvre relevant de la présente Question au 7 janvier 2022: Z.100, Z.101, Z.102, Z.103, Z.104, Z.105, Z.106, Z.107, Z.109, Z.110, Z.111, Z.119, Z.120, Z.121, Z.150, Z.151, Z.200, Z.450, Supplément Z.Suppl.1 et Guide de mise en œuvre Z.Imp100.

## 1.6 Motifs pour la tenue à jour des Recommandations OSI

Les travaux consacrés aux Recommandations de base relatives à l'interconnexion des systèmes ouverts (OSI) ont été achevés. Les systèmes fondés sur les Recommandations OSI peuvent être mis en œuvre pendant relativement longtemps. Lors de l'exploitation des systèmes mis en œuvre sur la base de ces Recommandations, on peut constater qu'il existe des erreurs techniques ou qu'il est souhaitable d'apporter des améliorations à ces Recommandations. Il est donc nécessaire de tenir à jour en permanence les Recommandations OSI de la série X.

Recommandations et Guides de mise en œuvre relevant de la présente Question au 7 janvier 2022: F.400, F.401, F.410, F.415, F.420, F.421, F.423, F.435, F.440, F.471, F.472, X.200, X.207, X.210, X.211, X.212, X.213, X.214, X.215, X.216, X.217, X.217bis, X.218, X.219, X.220, X.222, X.223, X.224, X.225, X.226, X.227, X.227bis, X.228, X.229, X.233, X.234, X.235, X.236, X.237, X.237bis, X.245, X.246, X.247, X.248, X.249, X.255, X.256, X.257, X.260, X.263, X.264, X.273, X.274, X.281, X.282, X.283, X.284, X.287, X.400, X.402, X.404, X.408, X.411, X.412, X.413, X.419, X.420, X.421, X.435, X.440, X.445, X.446, X.460, X.462, X.467, X.481, X.482, X.483, X.484, X.485, X.486, X.487, X.488, X.610, X.612, X.613, X.614, X.622, X.623, X.625, X.630, X.633, X.634, X.637, X.638, X.639, X.641, X.642, X.650, X.851, X.852, X.853, X.860, X.861, X.862, X.863, X.880, X.881, X.882 et Guide de mise en œuvre X.ImpOSI.

## 1.7 Motifs pour la tenue à jour des Recommandations ODP

Dans un système de télécommunication, la disponibilité de logiciels permettant un traitement réparti ouvert (ODP) revêt une importance fondamentale. Pour pouvoir assurer un traitement réparti ouvert, il faut normaliser des modèles de référence, des architectures, des fonctions, des interfaces et des langages (série UIT‑T X.900).

Recommandations relevant de la présente Question au 7 janvier 2022: X.901, X.902, X.903, X.904, X.906, X.910, X.911, X.920, X.930, X.931, X.950, X.952 et X.960.

# 2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

## 2.1 Sujets à étudier concernant les travaux sur les annuaires et les infrastructures PKI et PMI

Concernant les services d'annuaire*:*

a) Quelles nouvelles définitions de services ou quelles modifications dans la série F sont nécessaires pour déterminer comment les capacités actuelles peuvent être utilisées et quelles sont les nouvelles exigences concernant la Recommandation UIT‑T X.500?

b) Quelles améliorations faut-il apporter à la série E de Recommandations pour satisfaire aux nouvelles exigences des services?

c) Quelles améliorations faut-il apporter à l'annuaire pour satisfaire aux nouvelles exigences liées à l'infrastructure PKI?

d) Quelles sont les nouvelles exigences en matière de sécurité et de confidentialité des informations d'annuaire?

e) Quelles autres règles de codage pour la Recommandation UIT‑T X.500 (XML par exemple) peuvent être nécessaires pour améliorer encore l'utilité de la Recommandation UIT‑T X.500?

f) Quelles autres améliorations faut-il apporter aux certificats d'attributs et de clés publiques pour permettre leur utilisation dans divers environnements, par exemple les environnements à ressources limitées, les environnements de machine à machine et les grands réseaux?

g) Quelles autres améliorations faut-il apporter aux certificats d'attributs et de clés publiques pour accroître leur utilité dans des domaines tels que la biométrie, l'authentification, le contrôle d'accès et le commerce électronique?

h) Quelles modifications faut-il apporter aux Recommandations UIT‑T X.509 et UIT-T X.510 pour inclure les algorithmes à l'épreuve des attaques quantiques et les technologies des registres distribués?

Cette étude sera réalisée en collaboration avec l'ISO/CEI JTC 1/SC 6 dans le cadre du travail qu'il consacre à l'extension de la norme ISO/CEI 9594. Une coopération sera maintenue avec l'IETF, en particulier concernant le protocole LDAP et l'infrastructure PKI*.*

## 2.2 Sujets à étudier concernant les travaux sur l'ASN.1

a) Quelles améliorations faut-il apporter à la notation de syntaxe abstraite numéro un (ASN.1) et à ses règles de codage pour répondre aux besoins des futures applications?

b) Quelle collaboration, en dehors des accords en vigueur, faut-il établir avec d'autres organismes élaborant des normes de droit ou de fait pour que le travail de l'UIT-T sur l'ASN.1 continue d'occuper une place prééminente dans le domaine de la fourniture de notations pour la définition de protocoles?

Ces sujets seront étudiés en collaboration avec l'ISO/CEI JTC 1/SC 6.

## 2.3 Sujets à étudier concernant les identificateurs d'objet et leurs autorités d'enregistrement

a) Quels tutoriels sont nécessaires pour faciliter l'utilisation d'identificateurs d'objet dans divers environnements?

b) Quelles autorités d'enregistrement supplémentaires ou quelles procédures sont nécessaires pour faciliter les travaux effectués au titre de la présente Question et d'autres Questions?

c) Quelle collaboration, en dehors des accords en vigueur, faut-il établir avec d'autres organismes élaborant des normes de droit ou de fait pour que le travail de l'UIT-T sur les identificateurs d'objet continue d'occuper une place prééminente dans l'établissement de noms non ambigus?

Ces sujets seront étudiés en collaboration avec l'ISO/CEI JTC 1/SC 6.

## 2.4 Sujets à étudier concernant les travaux sur la notation TTCN

Quelles améliorations faut-il apporter à la notation TTCN-3 pour répondre aux besoins des futures applications?

Cette étude sera réalisée en collaboration avec l'ETSI TC MTS.

## 2.5 Maintenance des langages formels

Mise à jour permanente des Recommandations relatives au SDL, au profil UML, aux diagrammes MSC, à la notation URN et au langage CHILL.

## 2.6 Tenue à jour des Recommandations OSI

Mise à jour permanente des Recommandations sur l'architecture OSI et sur les différentes couches pour leur apporter les éventuelles améliorations nécessaires et pour corriger les erreurs signalées. Mise à jour permanente du service et des systèmes de traitement des messages, du transfert fiable, des opérations distantes, du service CCR et du traitement transactionnel OSI pour leur apporter les éventuelles améliorations nécessaires et pour corriger les erreurs signalées.

Il est hautement souhaitable de maintenir une collaboration et une liaison étroites avec les autres Commissions d'études et les autres groupes internationaux mettant en œuvre l'OSI pour garantir l'applicabilité la plus large possible des Recommandations correspondantes.

Le travail doit être effectué en collaboration avec l'ISO/CEI JTC 1 et ses sous-comités.

## 2.7 Tenue à jour des Recommandations ODP

Mise à jour permanente des Recommandations ODP.

Il est hautement souhaitable de maintenir une collaboration et une liaison étroites avec les autres Commissions d'études et les autres groupes internationaux mettant en œuvre l'ODP pour garantir l'applicabilité la plus large possible des Recommandations correspondantes.

Le travail doit être effectué en collaboration avec l'ISO/CEI JTC 1/SC 7/GT 19.

# 3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

## 3.1 Tâches concernant les travaux sur les annuaires et les infrastructures PKI et PMI

a) Mettre à jour l'annuaire en élaborant des rapports d'erreurs et des corrigenda techniques.

b) Déterminer les nouvelles exigences relatives à l'annuaire découlant des technologies existantes ou nouvelles.

c) Élaborer la neuvième édition de la série X.500 de Recommandations UIT‑T.

d) Définir les améliorations à apporter aux Recommandations UIT‑T X.509, X.510 et X.pki-em pour satisfaire aux nouvelles exigences, telles que les procédures automatiques applicables à la mise en place et à la maintenance des infrastructures PKI.

## 3.2 Tâches concernant les travaux sur l'ASN.1

a) Mettre à jour les Recommandations UIT‑T des séries X.680, X.690 et X.890 au cours de la période d'études pour répondre aux besoins des utilisateurs et élaborer de nouvelles versions si nécessaire.

b) Lorsqu'il est nécessaire d'améliorer le transfert de données, aider toutes les Commissions d'études à fournir des modules ASN.1 équivalents aux schémas XML définis dans les Recommandations UIT‑T (en vigueur ou en cours d'élaboration), notamment dans les cas où la largeur de bande est étroite.

c) Assurer le suivi des Recommandations | Normes internationales et corrigenda techniques approuvés en vue d'en faciliter la publication.

d) Traiter tous les rapports d'erreur et élaborer des corrigenda techniques si nécessaire.

e) Faire en sorte que toutes les notes de liaison relatives aux travaux sur l'ASN.1 soient traitées en temps voulu et de façon appropriée.

f) Élaborer les tutoriels ou pages web supplémentaires susceptibles d'aider les utilisateurs de l'ASN.1.

## 3.3 Tâches concernant les travaux sur les identificateurs d'objet et sur leurs autorités d'enregistrement

a) Mettre à jour les Recommandations UIT‑T des séries X.660 et X.670 au cours de la période d'études pour répondre aux besoins des utilisateurs et élaborer de nouvelles versions si nécessaire.

b) Assurer le suivi des Recommandations | Normes internationales et corrigenda techniques approuvés en vue d'en faciliter la publication.

c) Traiter tous les rapports d'erreur et élaborer des corrigenda techniques si nécessaire.

d) Faire en sorte que toutes les notes de liaison relatives aux travaux sur les identificateurs d'objet soient traitées en temps voulu et de façon appropriée.

e) Élaborer les tutoriels ou pages web supplémentaires susceptibles d'aider les utilisateurs d'identificateurs d'objet.

f) Obtenir l'accord de l'ISO/CEI JTC 1/SC 6 et de la CE 17 concernant les attributions supplémentaires d'identificateurs d'objet qui sont jugées nécessaires.

g) Examiner les candidatures pour les autorités d'enregistrement de chaque type de nom visé dans la Recommandation UIT-T X.660 | ISO/CEI 9834-1, proposer une organisation à la CE 17 en vue de sa désignation et informer l'ISO/CEI JTC 1/SC 6 de la candidature retenue au moyen d'une note de liaison.

h) Sous la responsabilité du chef du projet OID:

• fournir des indications générales aux utilisateurs d'identificateurs d'objet;

• promouvoir l'utilisation des identificateurs d'objet internationaux dans les autres Commissions d'études et dans les organismes de normalisation externes;

• aider les pays à établir et à maintenir une autorité d'enregistrement nationale pour les identificateurs d'objet (y compris les identificateurs d'objet internationaux).

## 3.4 Tâches concernant les travaux sur la notation TTCN

a) Actualiser les Recommandations relevant de la présente Question.

b) Promouvoir l'utilisation de la notation TTCN dans les autres Commissions d'études et dans les organismes de normalisation externes.

## 3.5 Tâches concernant les travaux sur la maintenance des langages formels

Apporter les modifications ou améliorations nécessaires aux Recommandations relatives au SDL, au profil UML, aux diagrammes MSC, à la notation URN et au langage CHILL. Mettre à jour le Guide de mise en œuvre SDL.

## 3.6 Tâches concernant la tenue à jour des Recommandations OSI

Apporter les modifications ou améliorations nécessaires aux Recommandations OSI sur la base des contributions reçues ou pour corriger les erreurs signalées. Mettre à jour le guide de mise en œuvre OSI.

## 3.7 Tâches concernant la tenue à jour des Recommandations ODP

Apporter les modifications ou améliorations nécessaires aux Recommandations ODP sur la base des contributions reçues ou pour corriger les erreurs signalées.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 17 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>).

# 4 Relations

Grandes orientations du SMSI:

– C5

Objectifs de développement durable:

– 8 ([Travail décent et croissance économique](http://www.un.org/development/desa/disabilities/envision2030-goal8.html))

– 9 ([Industrie, innovation et infrastructure](http://www.un.org/development/desa/disabilities/envision2030-goal9.html))

Recommandations:

– Série H.200, H.323, série H.350, T.120, série X.600-X.609, série X.700, série X.800‑X.849, série Z

Questions:

– Toutes les Questions de l'UIT-T relatives aux Recommandations ci-dessus et la Question 14/17 concernant l'infrastructure PKI répartie

Commissions d'études:

– CE 2, 9, 11, 13, 15, 16 et 20 de l'UIT-T et toutes les Commissions d'études qui utilisent les solutions d'annuaire, la notation ASN.1, les OID et les tests de conformité et d'interopérabilité, ou qui ont besoin de les utiliser

Organismes de normalisation:

– Internet Engineering Steering Group (IESG); Internet Engineering Task Force (IETF); CEI/TC 57; ISO/CEI JTC 1/SC 6, 7, 27 et 31, ISO TC 68, 204; Organization for the Advancement of Structured Information Standards (OASIS); Object Management Group (OMG); World Wide Web Consortium (W3C); Institut européen des normes de télécommunication (ETSI) (TC MTS); ISO/CEI JTC 1 et ses sous-comités qui utilisent les langages UIT de conception de systèmes

Autres organismes:

– Union postale universelle (UPU); SDL Forum Society

QUESTION 13/17

Sécurité des systèmes de transport intelligents

(Suite de la Question 13/17)

# 1 Motifs

Les systèmes de transport intelligents (ITS), qui comprennent les systèmes de conduite autonome, offrent divers types d'applications visant à renforcer la sécurité routière, à réduire l'impact des transports sur l'environnement, à améliorer la gestion de la circulation et à permettre aux utilisateurs publics et commerciaux de tirer le meilleur parti des avantages liés au secteur des transports.

Les systèmes ITS font appel à divers types de communications dans les véhicules (par exemple, de véhicule à dispositif nomade), entre véhicules (par exemple, de véhicule à véhicule (V2V)) et entre un véhicule et un emplacement fixe (par exemple, de véhicule à infrastructure (V2I)), c'est-à-dire les communications entre un véhicule et tout autre élément (V2X). Les technologies de l'information et de la communication (TIC) sont utilisées pour la mise en œuvre des systèmes ITS dans les transports routiers, ferroviaires, maritimes et aériens, mais aussi dans les systèmes de navigation.

Les systèmes de conduite automatisée et de conduite assistée comprennent plusieurs composantes de systèmes où la perception, la prise de décision et la conduite du véhicule sont confiées à des éléments électroniques et à des machines plutôt qu'à un conducteur humain et qui prévoient l'application du principe d'automatisation à la circulation routière.

Dans l'environnement des systèmes ITS, qui comprennent les systèmes de conduite autonome et de conduite assistée, les vulnérabilités d'un véhicule peuvent être transmises à d'autres véhicules étant donné qu'ils sont connectés entre eux. Il est donc nécessaire de gérer les vulnérabilités des systèmes de communication V2X et d'y remédier afin qu'elles n'affectent pas un trop grand nombre de véhicules.

Les dispositifs électroniques embarqués à bord des véhicules, notamment les unités de commande électroniques (ECU) et les systèmes de télépéage (ETC), sont de plus en plus sophistiqués. Il en résulte qu'une mise à jour appropriée des modules logiciels présents dans ces dispositifs est indispensable afin d'améliorer la performance et la sécurité.

La Recommandation UIT-T X.1373, approuvée en mars 2017, porte sur la capacité de mise à jour logicielle sécurisée pour les dispositifs de communication des systèmes ITS. Elle est en cours de révision.

La normalisation de solutions de sécurité complètes optimales est essentielle pour l'environnement des systèmes ITS. Du fait de certaines caractéristiques propres aux communications à bord des véhicules, garantir la sécurité est une tâche particulièrement difficile qui devrait faire l'objet d'études.

Recommandations relevant de la présente Question au 7 janvier 2022: X.1371, X.1372, X.1373, X.1374, X.1375 et X.1376.

Textes en cours d'élaboration au 7 janvier 2022: X.1373rev, X.edrsec, X.eivnsec, X.evtol-sec, X.fstiscv, X.idse, X.ipscv, X.itssec-5, X.rsu-sec et X.srcd.

# 2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

a) Comment identifier et définir les aspects relatifs à la sécurité (par exemple, l'architecture et les sous-systèmes de sécurité) dans l'environnement des systèmes ITS et des systèmes de conduite autonome et de conduite assistée?

b) Comment identifier et traiter les menaces et les vulnérabilités dans les services et les réseaux liés aux systèmes ITS et aux systèmes de conduite autonome et de conduite assistée?

c) Quelles sont les exigences de sécurité (par exemple, en termes d'identification et d'authentification) nécessaires pour atténuer les menaces dans l'environnement des systèmes ITS et des systèmes de conduite autonome et de conduite assistée?

d) Quelles technologies permettent de renforcer la sécurité des services et des réseaux ITS?

e) Comment assurer et maintenir une interconnectivité sécurisée entre les entités dans l'environnement des systèmes ITS et des systèmes de conduite autonome et de conduite assistée?

f) Quelles techniques, quels mécanismes et quels protocoles de sécurité sont nécessaires pour les services et les réseaux liés aux systèmes ITS et aux systèmes de conduite autonome et de conduite assistée?

g) Quelles sont les solutions de sécurité globalement acceptables pour les services et les réseaux (basés sur les réseaux de télécommunication/TIC) liés aux systèmes ITS et aux systèmes de conduite autonome et de conduite assistée?

h) Quelles sont les bonnes pratiques ou les lignes directrices relatives à la sécurité des systèmes ITS et des systèmes de conduite autonome et de conduite assistée?

i) Comment exploiter les technologies reposant sur l'intelligence artificielle et sur l'apprentissage automatique pour assurer la sécurité et la confiance concernant les systèmes ITS et les systèmes de conduite autonome et de conduite assistée?

j) Quels mécanismes de protection et de gestion des informations d'identification personnelle (PII) sont nécessaires pour les services ITS?

# 3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

a) Élaborer un ensemble de Recommandations définissant des solutions de sécurité complètes pour les systèmes ITS et pour les systèmes de conduite autonome et de conduite assistée.

b) Mener des études complémentaires pour définir les aspects de sécurité des services et des réseaux (basés sur les réseaux de télécommunication/TIC) liés aux systèmes ITS et aux systèmes de conduite autonome et de conduite assistée.

c) Étudier et recenser les problèmes et menaces de sécurité dans les systèmes ITS et dans les systèmes de conduite autonome et de conduite assistée.

d) Étudier et recenser les exigences et les cas d'utilisation concernant les services et les applications propres aux systèmes ITS et aux systèmes de conduite autonome et de conduite assistée.

e) Étudier et élaborer des mécanismes, des protocoles et des technologies de sécurité pour les systèmes ITS et les systèmes de conduite autonome et de conduite assistée.

f) Étudier et définir des profils, un système d'authentification hiérarchique et un mécanisme de sécurité pour les services et les applications propres aux systèmes ITS et aux systèmes de conduite autonome et de conduite assistée.

g) Étudier et élaborer des applications sur la base d'algorithmes de chiffrement et de déchiffrement efficaces pour accélérer le déplacement des nœuds de réseau et pour modifier dynamiquement les topologies de réseau.

h) Étudier et élaborer des technologies d'enregistrement des données d'incident dans le contexte des systèmes ITS et des systèmes de conduite autonome et de conduite assistée.

i) Étudier et définir des mécanismes d'interconnectivité sécurisée pour les systèmes ITS et les systèmes de conduite autonome et de conduite assistée dans un environnement de télécommunication.

j) Étudier et recenser les problèmes de protection des informations PII et les menaces associées dans les systèmes ITS et dans les systèmes de conduite autonome et de conduite assistée.

k) Étudier et définir des mécanismes de protection et de gestion des informations PII pour les systèmes ITS et pour les systèmes de conduite autonome et de conduite assistée.

l) Étudier et élaborer des technologies de sécurité basées sur l'intelligence artificielle/l'apprentissage automatique pour les systèmes ITS et les systèmes de conduite autonome et de conduite assistée.

m) Étudier et mettre à jour les projets existants de Recommandations X.1373rev, X.itssec‑5, X.srcd, X.edrsec, X.eivnsec, X.fstiscv, X.ipscv, X.rsu-sec, X.evtol-sec.

n) Collaborer avec les organismes de normalisation concernés pour élaborer conjointement des Recommandations.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 17 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>).

# 4 Relations

Grandes orientations du SMSI:

– C5

Objectifs de développement durable:

– 8 ([Travail décent et croissance économique](http://www.un.org/development/desa/disabilities/envision2030-goal8.html))

– 9 ([Industrie, innovation et infrastructure](http://www.un.org/development/desa/disabilities/envision2030-goal9.html))

– 11 ([Villes et communautés durables](http://www.un.org/development/desa/disabilities/envision2030-goal11.html))

Recommandations:

– Série X et autres Recommandations se rapportant à la sécurité

Questions:

– Questions 1/17, 2/17, 3/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17 et 15/17 de l'UIT-T

Commissions d'études et groupes spécialisés:

– CE 11, 13, 16 et 20 de l'UIT-T

– GT 5A de l'UIT-R

– Collaboration sur les normes de communication pour les systèmes ITS (CITS)

– Groupe spécialisé de l'UIT-T sur le multimédia dans les véhicules (FG-VM)

Organismes de normalisation:

– ISO TC 22 et 204

– ISO/CEI JTC 1/SC 6 et 27

– IETF WG ITS

– IEEE 802.11 WG et 1609 WG

– SAE International (notamment: Vehicle Cybersecurity Systems Engineering Committee, Connected Vehicles Steering Committee et DSRC Technical Standard Committee); ETSI TC ITS; W3C Automotive WG.

Autres organismes:

– GSMA

– ATIS; CCSA; TIA; TTA; TTC

– Groupe de travail 29 de la Commission économique des Nations Unies pour l'Europe (CEE-ONU) et organes subsidiaires (par exemple, Équipe spéciale pour la cybersécurité (TFCS))

– Automotive Grade Linux (AGL)

QUESTION 14/17

Sécurité de la technologie des registres distribués (DLT)

(Suite de la Question 14/17)

# 1 Motifs

La technologie des registres distribués (DLT), dont l'application la plus notable est la chaîne de blocs, repose sur un nouveau type de registres sécurisés qui sont partagés, dupliqués et synchronisés de manière distribuée. Les données contenues dans les registres distribués sont contrôlées par plusieurs parties.

En tant que technologie de base de données distribuée spécifique, la technologie DLT est intrinsèquement résistante à la modification des données. Une fois que les données sont enregistrées dans un bloc, elles ne peuvent pas être modifiées rétroactivement. Cette caractéristique importante de la technologie DLT est devenue notoire suite au succès des premières applications numériques de crypto-monnaie, à savoir le Bitcoin.

La technologie DLT compte désormais parmi les technologies de rupture qui ouvrent des possibilités immenses pour transformer notre économie, notre culture et notre société. Elle permet d'assurer des applications financières/non financières décentralisées novatrices qui éliminent la nécessité de recourir à des tierces parties intermédiaires. Avec cette technologie, une nouvelle infrastructure de gestion des données sera mise en place, qui entraînera une véritable révolution dans les secteurs faisant appel aux télécommunications (par exemple la banque, la finance, les administrations publiques, les services de santé et la logistique à large échelle).

La technologie des registres distribués aura des retombées considérables pour les utilisateurs des télécommunications et les entreprises du secteur, y compris les fournisseurs de services de télécommunication.

Il est nécessaire d'identifier les rôles et les responsabilités des utilisateurs, des opérateurs et des fournisseurs de services dans le domaine des télécommunications concernant les aspects liés à la sécurité de l'environnement DLT.

La normalisation de solutions de sécurité complètes optimales est essentielle pour la technologie DLT, qui comporte de nombreux cas d'utilisation dans divers secteurs, y compris celui des télécommunications. Du fait de certaines caractéristiques propres à la technologie DLT, garantir la sécurité est une tâche particulièrement difficile qui devrait faire l'objet d'études.

Recommandations relevant de la présente Question au 7 janvier 2022: X.1400, X.1401, X.1402, X.1403, X.1404, X.1405, X.1406, X.1407 et X.1408.

Textes en cours d'élaboration au 7 janvier 2022: X.sa-dsm, X.sc-dlt, X.srscm-dlt, X.ss-dlt et TR.qs‑dlt.

# 2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

a) Comment identifier et définir les aspects relatifs à la sécurité (par exemple, l'architecture et les sous-systèmes) sur la base de certains fondements (termes et définitions, concepts et taxonomie, cas d'utilisation) de l'environnement DLT?

b) Comment traiter les menaces et vulnérabilités dans les applications et les services reposant sur la technologie DLT?

c) Quelles sont les exigences de sécurité nécessaires pour atténuer les menaces dans un environnement DLT?

d) Quelles technologies de sécurité peuvent être utilisées pour les applications et les services reposant sur la technologie DLT?

e) Comment assurer et maintenir une interconnectivité sécurisée entre les entités dans un environnement DLT?

f) Quelles techniques, quels mécanismes et quels protocoles de sécurité sont nécessaires pour les applications et les services reposant sur la technologie DLT?

g) Quelles sont les solutions de sécurité globalement acceptables pour les applications et les services reposant sur la technologie DLT et fondés sur les réseaux de télécommunication/TIC?

h) Quelles sont les bonnes pratiques ou les lignes directrices relatives à la sécurité pour les applications et les services reposant sur la technologie DLT?

i) Quels mécanismes de protection des informations d'identification personnelle (PII) et de gestion de la sécurité des informations sont nécessaires pour les applications et les services reposant sur la technologie DLT?

j) Comment la technologie DLT peut-elle être utilisée pour renforcer la sécurité?

k) Comment analyser, évaluer et garantir la sécurité de la technologie DLT?

l) Avec quelles parties prenantes la CE 17 devrait-elle collaborer?

# 3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

a) Analyser les lacunes des travaux qui sont en cours au sein d'autres organismes concernant la sécurité des technologies des registres distribués.

b) Mener des études complémentaires pour définir les aspects de sécurité des applications et des services reposant sur la technologie DLT et fondés sur les réseaux de télécommunication/TIC.

c) Étudier les fondements tels que les termes, les définitions, les concepts, la taxonomie et les cas d'utilisation qui sont liés à la sécurité et à la protection des informations PII dans les réseaux DLT.

d) Étudier et recenser les problèmes et menaces de sécurité dans les applications et les services reposant sur la technologie DLT.

e) Étudier et élaborer des mécanismes, des protocoles et des technologies de sécurité pour les applications et les services reposant sur la technologie DLT.

f) Étudier et définir des mécanismes d'interconnectivité sécurisée pour les applications et les services reposant sur la technologie DLT.

g) Étudier et recenser les problèmes de protection des informations PII et les menaces associées dans les applications et les services reposant sur la technologie DLT.

h) Étudier et élaborer un système de gestion des informations destiné aux entités qui fournissent des applications et des services reposant sur la technologie DLT.

i) Étudier et définir des orientations concernant l'utilisation de la technologie DLT afin de renforcer la sécurité.

j) Étudier et définir des orientations pour analyser, évaluer et garantir la sécurité de la technologie DLT.

k) Élaborer un ensemble de Recommandations définissant des solutions de sécurité complètes pour les applications et les services reposant sur la technologie DLT.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 17 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>).

# 4 Relations

Grandes orientations du SMSI:

– C5

Objectifs de développement durable:

– 8 ([Travail décent et croissance économique](http://www.un.org/development/desa/disabilities/envision2030-goal8.html))

– 9 ([Industrie, innovation et infrastructure](http://www.un.org/development/desa/disabilities/envision2030-goal9.html))

– 11 ([Villes et communautés durables](http://www.un.org/development/desa/disabilities/envision2030-goal11.html))

Recommandations:

– Série X et autres Recommandations se rapportant à la sécurité

Questions:

– Questions 1/17, 2/17, 3/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17 et 15/17 de l'UIT‑T

Commissions d'études:

– CE 5, 11, 13, 16 et 20 de l'UIT-T

Organismes de normalisation:

– ISO TC 307

– ISO/CEI JTC 1/SC 27

Autres organismes:

– GSMA; W3C, IEEE

– Commission économique des Nations Unies pour l'Europe (CEE-ONU); Initiative mondiale en faveur de l'inclusion financière (FIGI)

– ATIS; CCSA; TIA; TTA; TTC

QUESTION 15/17

Sécurité relative aux nouvelles technologies, y compris la sécurité quantique

(Suite de la Question 15/17)

# 1 Motifs

La CE 17 reconnaît la nature dynamique des études sur la sécurité, qui dépendent fortement du bras de fer entre les auteurs d'attaque et les défenseurs, mais aussi des retombées des innovations exploitées par les deux camps. Par conséquent, on voit régulièrement apparaître de nouvelles technologies de sécurité et, pour certaines d'entre elles, une normalisation à l'échelle mondiale est nécessaire.

Par nature, il est impossible d'anticiper ce qui adviendra et quand, et la CE 17 a donc pris l'initiative de mettre en place un mécanisme d'incubation (TP.inno), qui permet d'étudier avec plus de souplesse les nouveaux domaines liés à la sécurité. Le but est de sécuriser les nouveaux services et les nouvelles applications reposant sur les télécommunications/TIC.

Ce mécanisme d'incubation permet à la CE 17 de définir efficacement de nouveaux sujets d'étude dans ces domaines et il favorise l'élaboration de textes non normatifs (documents techniques et rapports techniques). Cette bonne pratique a fait ses preuves et laisse aux participants aux travaux de la CE 17 le temps de se familiariser avec ces nouveaux domaines et aux nouveaux arrivants le temps de mieux connaître les procédures et l'environnement propres à la CE 17 et à l'UIT-T. Il peut apparaître, au moment de définir un nouveau sujet d'étude, qu'une nouvelle technologie de sécurité se rapproche davantage d'une Question existante, de par sa nature. Le sujet d'étude concerné peut donc être transféré afin d'améliorer la cohérence, l'efficacité et la qualité des travaux de la CE 17.

Ce mécanisme d'incubation permet également d'identifier les tendances concernant les nouvelles technologies de sécurité qui sont abordées au titre la présente Question. On parle de nouvelles technologies dans divers cas de figure, notamment lorsque:

– la technologie concerne un thème nouveau. C'est le cas par exemple pour la sécurité quantique, les calculs multi-parties sécurisés, le chiffrement homomorphe ou encore les solutions de sécurité pouvant être identifiées pour la robotique, etc.;

– le thème n'est pas nouveau, mais c'est la première fois qu'il fait l'objet d'une normalisation à l'échelle mondiale. C'est le cas par exemple pour l'analyse des logiciels malveillants, la prévention de la perte de données, etc.;

– la technologie est apparue pour remédier aux lacunes en termes d'architecture opérationnelle de la sécurité qui ne relevaient d'aucune question existante. C'est le cas par exemple des produits de sécurité eux-mêmes;

– la technologie est apparue pour régler les problèmes importants d'intégration et de composition. Elle a donné lieu à de nouvelles solutions transversales, à de nouveaux modèles de données de sécurité, etc.

L'un des nouveaux domaines identifiés grâce au mécanisme d'incubation est la sécurité quantique. L'apparition d'ordinateurs quantiques à grande échelle implique potentiellement une perturbation conséquente des systèmes de télécommunication classiques qui font appel aux TIC, mais elle présente également des risques importants en matière de sécurité.

De fait, les méthodes de cryptographie utilisées actuellement à des fins de sécurité reposent sur des problèmes difficiles à résoudre par le calcul: les problèmes de logarithme discret et les problèmes de factorisation d'entiers. Ces problèmes sont considérés comme étant difficiles à résoudre en un temps raisonnable, compte tenu des architectures actuelles des ordinateurs disponibles aujourd'hui et à moyen terme. Or la cryptographie à clé publique (par clés asymétriques) est essentielle pour l'authentification sur les réseaux publics. De par leur nature, les ordinateurs quantiques sont capables de résoudre des problèmes de logarithme discret et de factorisation d'entiers assez rapidement et ils sont donc à même, par effet d'entraînement, de briser les fondements sur lesquels repose la cryptographie actuellement, menaçant ainsi l'un des piliers fondamentaux du cyberenvironnement et de l'environnement numérique actuels.

La distribution de clés quantiques (QKD) permet à deux parties de générer une clé secrète aléatoire partagée dont elles seules ont connaissance et qui peut être utilisée pour chiffrer et déchiffrer des messages grâce à des algorithmes de cryptographie classiques. La distribution de clés quantiques est limitée pour deux raisons, qui entraînent des problèmes en termes de topologie et d'intégration des réseaux: a) il s'agit d'une distribution point à point ne pouvant être appliquée qu'à deux parties, A et B, et b) sa portée est limitée aux réseaux terrestres. Afin de surmonter ces limites, les réseaux de distribution de clés quantiques ont été introduits dans le secteur. Ils se caractérisent par 1) un ensemble de nœuds reliés entre eux via des systèmes de distribution de clés quantiques point à point et par 2) un système de gestion partagé entre tous les nœuds de distribution de clés quantiques et intégré à chacun d'entre eux. Ce système de gestion a pour but de distribuer des clés secrètes entre deux nœuds, ou plus, qui font partie du même réseau de distribution de clés quantiques mais qui ne sont pas nécessairement reliés directement entre eux. À l'heure actuelle, les systèmes de distribution de clés quantiques commerciaux sont suffisamment stables et aboutis, et il est donc possible d'envisager l'établissement de réseaux de distribution de clés quantiques à grande échelle. Il existe plusieurs initiatives émanant d'entreprises et d'institutions qui visent à développer les réseaux de distribution de clés quantiques. Toutefois, il n'existe pas de norme largement reconnue sur ce qui caractérise un système de distribution de clés quantiques.

En outre, les nombres aléatoires sont un élément capital de l'ingénierie et ils jouent un rôle important dans la cryptographie. Ce caractère aléatoire inhérent à la mécanique quantique fait des systèmes quantiques une source typique d'entropie. La génération quantique de nombres aléatoires est l'une des technologies quantiques les plus abouties et il existe de nombreuses méthodes de génération possibles.

En résumé, la sécurité quantique vise à protéger les communications contre les attaques d'ordinateurs quantiques. La mise en œuvre de la sécurité quantique nécessite plusieurs éléments clés, notamment la distribution de clés quantiques et un générateur quantique de nombres aléatoires. En outre, il est important de garantir l'interopérabilité entre ces éléments clés et leurs fonctionnalités afin qu'ils puissent être largement utilisés dans les réseaux de télécommunication réels.

Par ailleurs, il est essentiel que la CE 17 mène des études sur la sécurité quantique, qui protège contre les attaques quantiques.

Recommandations et documents/rapports techniques relevant de la présente Question au 7 janvier 2022: X.1702, X.1710, X.1712, X.1714, X.1770 et documents techniques TP.inno, TP.sgstruct et TR.sec-qkd.

Textes en cours d'élaboration au 7 janvier 2022: Corrigendum de la Recommandation X.1712, X.icd-schemas, X.sec\_QKDN\_AA, X.sec\_QKDN\_CM, X.sec\_QKDN\_intrq, X.sec-QKDN-tn, TR.hybsec-qkdn, TR.sec-ai et TR.sgfdm.

# 2 Question

Les sujets à étudier sont notamment les suivants (la liste n'est pas exhaustive):

a) Quelles sont les nouvelles technologies de sécurité qui se font jour?

b) Quelles sont les catégories de nouvelles technologies de sécurité?

c) Comment développer de manière sûre les nouvelles technologies de sécurité?

d) Quels sont les mécanismes les plus efficaces pour mettre en œuvre un mécanisme d'incubation?

e) Quels sont les enjeux de l'apparition des ordinateurs quantiques à grande échelle et quelles en sont les incidences sur les communications classiques?

f) Quels sont les éléments clés pour l'instauration de la sécurité quantique?

g) Quelle stratégie de transition adopter pour instaurer la sécurité quantique?

h) Comment traiter les menaces et les vulnérabilités concernant la sécurité quantique?

i) Quelles sont les exigences de sécurité nécessaires pour atténuer les menaces concernant la sécurité quantique?

j) Quelles technologies de sécurité permettent d'assurer la sécurité quantique?

k) Comment assurer et maintenir une interconnectivité sécurisée entre les entités concernant la sécurité quantique?

l) Quelles exigences, quelles techniques, quels mécanismes et quels protocoles de sécurité sont nécessaires pour la sécurité quantique?

m) Quelles sont les solutions de sécurité globalement acceptables pour la sécurité quantique, qui est fondée sur les réseaux de télécommunication/TIC?

n) Quelles sont les bonnes pratiques ou les lignes directrices applicables à la sécurité quantique?

# 3 Tâches

Les tâches sont notamment les suivantes (la liste n'est pas exhaustive):

a) Recenser les nouvelles technologies de sécurité qui se font jour.

b) Recenser les catégories de nouvelles technologies de sécurité afin de finaliser la stratégie pour l'étude de la Question M.

c) Transférer éventuellement le nouveau sujet d'étude à une autre Question s'il apparaît, lors de son examen, qu'il se rapproche davantage d'une Question existante.

d) Exploiter le mécanisme d'incubation pour l'étude des nouveaux domaines confiés à la CE 17 de l'UIT-T.

e) Élaborer un ensemble de Recommandations techniques définissant des solutions de sécurité complètes pour instaurer la sécurité quantique.

f) Mener des études pour identifier les aspects de la sécurité quantique, qui est fondée sur l'infrastructure de télécommunication/TIC.

g) Étudier et recenser les problèmes et menaces de sécurité concernant la sécurité quantique.

h) Étudier et élaborer des exigences, des mécanismes, des protocoles et des technologies de sécurité pour la sécurité quantique.

i) Étudier et définir des mécanismes d'interconnectivité sécurisée pour la sécurité quantique.

j) Étudier et élaborer un système de gestion des informations destiné aux entités qui garantissent la sécurité quantique.

L'état actuel d'avancement des travaux au titre de cette Question est indiqué dans le programme de travail de la CE 17 (<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>).

# 4 Relations

Grandes orientations du SMSI:

– C5

Objectifs de développement durable:

– 8 ([Travail décent et croissance économique](http://www.un.org/development/desa/disabilities/envision2030-goal8.html))

– 9 ([Industrie, innovation et infrastructure](http://www.un.org/development/desa/disabilities/envision2030-goal9.html))

– 11 ([Villes et communautés durables](http://www.un.org/development/desa/disabilities/envision2030-goal11.html))

Recommandations:

– Série X et autres Recommandations se rapportant à la sécurité

Questions:

– Questions 1/17, 2/17, 3/17, 4/17, 6/17, 7/17, 8/17, 10/17, 11/17, 13/17 et 14/17 de l'UIT‑T

Commissions d'études:

– CE 2, 3, 5, 9, 11, 12, 13, 15, 16 et 20 de l'UIT-T

Organismes de normalisation:

– ETSI TC Cyber, ISG-QKD

– ISO/CEI JTC 1/SC 27

– OASIS

– IETF

Autres organismes:

– GSMA; ATIS; CCSA; TIA; TTA; TTC

\_\_\_\_\_\_\_\_\_\_\_\_\_\_